



LevelOne

WBR-3402TX

1W,4L 11g Wireless ADSL Router
w/VPN/Printer Server(USB)

User`s Manual

Table of Contents

Chapter 1	Introduction	4
	Functions and Features	4
	Packing List	6
Chapter 2	Hardware Installation.....	7
	2.1 Panel Layout	7
	2.2 Procedure for Hardware Installation.....	8
Chapter 3	Network Settings and Software Installation	10
	3.1 Make Correct Network Settings of Your Computer.....	10
	3.2 Install the Software into Your Computers.....	11
Chapter 4	Configuring ADSL Wireless Broadband Router	13
	4.1 Start-up and Log in	14
	4.2 Status	15
	4.3 Wizard.....	16
	4.4 Basic Setting	17
	4.5 Forwarding Rules	33
	4.6 Security Settings	37
	4.6.1 Packet Filter.....	38
	4.6.2 Domain Filter.....	42
	4.6.3 URL Blocking.....	44
	4.6.4 MAC Address Control	46
	4.6.5 VPN setting.....	48
	4.6.6 Miscellaneous Items	54
	4.7 Advanced Setting	55
	4.7.1 ADSL Modem Performance Setting	56
	4.7.2 System Time	58
	4.7.3 System Log	59
	4.7.4 Dynamic DNS.....	61
	4.7.5 SNMP Setting	63
	4.7.6 Routing Table.....	65
	4.7.7 Schedule Rule	67
	4.8 Toolbox	71
	4.8.1 View Log	72
	4.8.2 Firmware Upgrade	73
	4.8.3 Backup Setting.....	74
	4.8.4 Reset to default	74
	4.8.5 Reboot.....	74

4.8.6 Miscellaneous Items	75
Chapter 5 Print Server	76
5.1 Configuring on Windows 95/98 Platforms	76
5.2 Configuring on Windows NT Platforms	79
5.3 Configuring on Windows 2000 and XP Platforms.....	80
5.4 Configuring on Unix-like based Platforms	85
5.5 Configuring on Apple PC	90
Appendix A TCP/IP Configuration for Windows 95/98	91
Appendix B Win 2000/XP IPSEC Setting guide	97
Appendix C PPTP and L2TP Configurations.....	133
Appendix D 802.1x Setting.....	139
Appendix E FAQ and Troubleshooting.....	145
Reset to factory Default	145
TFTP Mode.....	145

Chapter 1 Introduction

Congratulations on your purchase of LevelOne WBR-3402 ADSL Wireless Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

Functions and Features

Router Basic functions

- **Auto-sensing Ethernet Switch**
Equipped with a 4-port auto-sensing Ethernet switch.
- **Printer sharing**
Embedded a print server to allow all of the networked computers to share one printer.
Built-in USB host to connect to USB printer for printer sharing
- **Wan type supported**
The router supports some wan types, Ethernet Over ATM(RFC 1483 Bridged) without NAT, Ethernet Over ATM(RFC 1483 Bridged) with NAT, IP over ATM(RFC 1483 Routed), Classical Ip over ATM(RFC 1577), PPP over ATM (RFC 2364), PPP over Ethernet(RFC 2516).
- **Firewall**
All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**
All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**
Configurable through any networked computer's web browser using Netscape or Internet Explorer.
- **Virtual Server supported**
Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **User-Definable Application Sensing Tunnel**
User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.
- **DMZ Host supported**
Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function

correctly.

- **Statistics of WAN Supported**

Enables you to monitor inbound and outbound packets

Wireless functions

- **High speed for wireless LAN connection**

Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

- **Roaming**

Provides seamless roaming within the IEEE 802.11b(11M) and IEEE 802.11g(54M) WLAN infrastructure.

- **IEEE 802.11b compatible (11M)**

Allowing inter-operation among multiple vendors.

- **IEEE 802.11g compatible (54M)**

Allowing inter-operation among multiple vendors.

- **Auto fallback**

54M, 48M,36M, 24M, 18M,12M, 6M data rate with auto fallback in 802.11g mode.

11M, 5.5M, 2M, 1M data rate with auto fallback in 802.11b mode.

Security functions

- **Packet filter supported**

Packet Filter allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Domain Filter Supported**

let you prevent users under this device from accessing specific URLs.

- **URL Blocking Supported**

URL Blocking can block hundreds of websites connection by simply a **keyword**.

- **VPN Servers**

The router has three vpn server, IPSEC (Dynamic vpn),PPTP,L2TP.

- **VPN Pass-through**

The router also supports vpn pass-through.

- **802.1X supported**

When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

- **SPI Mode Supported**

When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.

- **DoS Attack Detection Supported**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

Advanced functions

- **System time Supported**

Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

The router can send its info by mail.

- **Dynamic dns Supported**

At present, the router has 3 ddns, dyndns, TZO.com and dhs.org.

- **SNMP Supported**

Because SNMP this function has many versions, anyway, the router supports V1 and V2c.

- **Routing Table Supported**

Now, the router supports static routing and two kinds of dynamic routing RIP1 and RIP2.

- **Schedule Rule supported**

Customers can control some functions, like virtual server and packet filters when to access or when to block.

Other functions

- **UPNP (Universal Plug and Play) Supported**

The router also supports this function. The applications: X-box, Msn Messenger.

Packing List

- WBR-3402, Wireless ADSL Router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable

Chapter 2 Hardware Installation

2.1 Panel Layout

2.1.1. Front Panel



Figure 2-1 Front Panel

LED:

LED	Function	Color	Status	Description
POWER	Power indication	Green	On	Power is being applied to this product.
STATUS	System status	Green	Blinking	This product is functioning properly.
Show-tme	ADSL status1	Green	On	The ADSL is linked.
			Blinking	This router is trying to connect to your ISP
ADSL-Act	ADSL status2	Green	Blinking	The ADSL is sending or receiving data.
WLAN	Wireless activity	Green	Blinking	Sending or receiving data via wireless
L1~L4	Link status	Green	On	An active station is connected to the corresponding LAN port.
			Blinking	The corresponding LAN port is sending or receiving data.

2.1.2. Rear Panel



Figure 2-2 Rear Panel

Ports:

Port	Description
5VDC	Power inlet: DC 5V, 2A
ADSL	the port where you will connect your phone jack..
Port 1-4	the ports where you will connect networked computers and other devices.
USB	USB Ports for USB printer.

2.2 Procedure for Hardware Installation

1. Decide where to place your WBR-3402, Wireless ADSL Router

You can place your ADSL Wireless Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your ADSL Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

2. Setup LAN connection

- a. Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
- b. Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

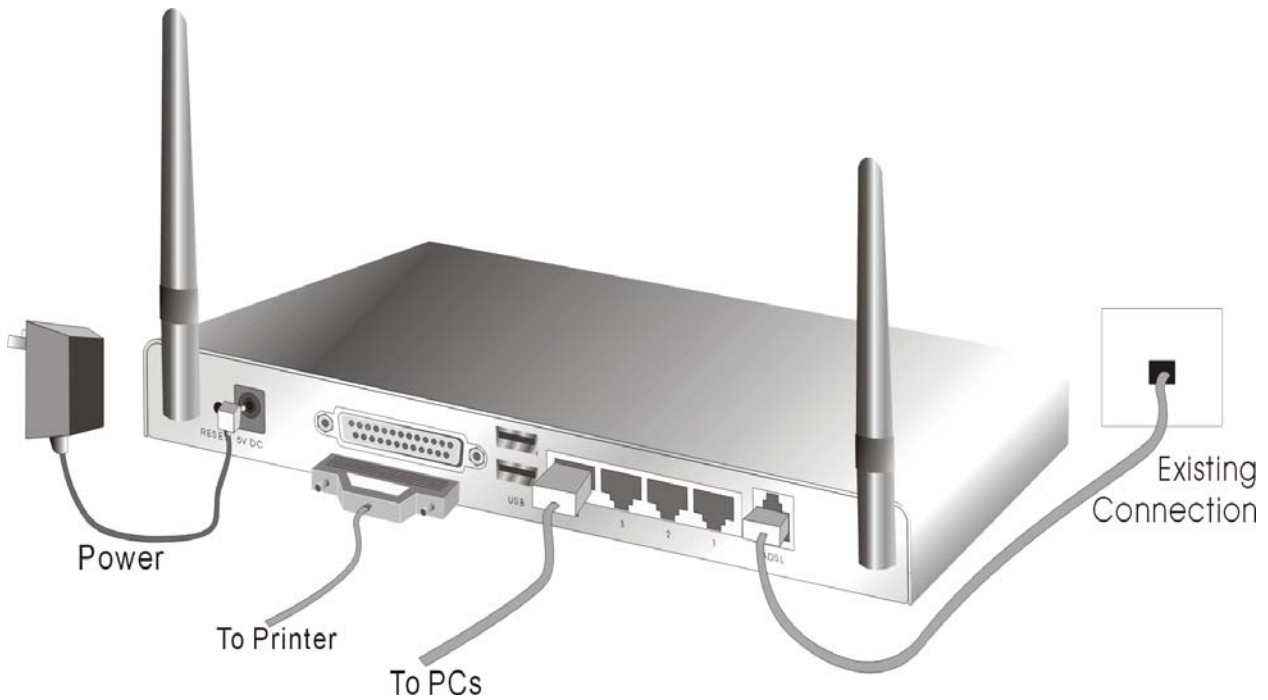


Figure 2-3 Setup of LAN and WAN connections for this product.

3. Setup ADSL connection

Prepare a telephone cable for connecting this product to your ISP. Figure 2-3 illustrates the ADSL connection.

4. Connecting this product with your printer

Use the printer cable to connect your printer to the USB printer port of this product.

5. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators STATUS will be lighted ON for about 10 seconds, and then STATUS will be flashed 3 times to indicate that the self-test operation has finished. Finally, the STATUS will be continuously flashed once per second to indicate that this product is in normal operation.

Chapter 3 Network Settings and Software Installation

To use WBR-3402 correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000).

3.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,
2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

ping 192.168.123.254

If the following messages appear:

Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time=2ms TTL=64

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

Pinging 192.168.123.254 with 32 bytes of data:

Request timed out.

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

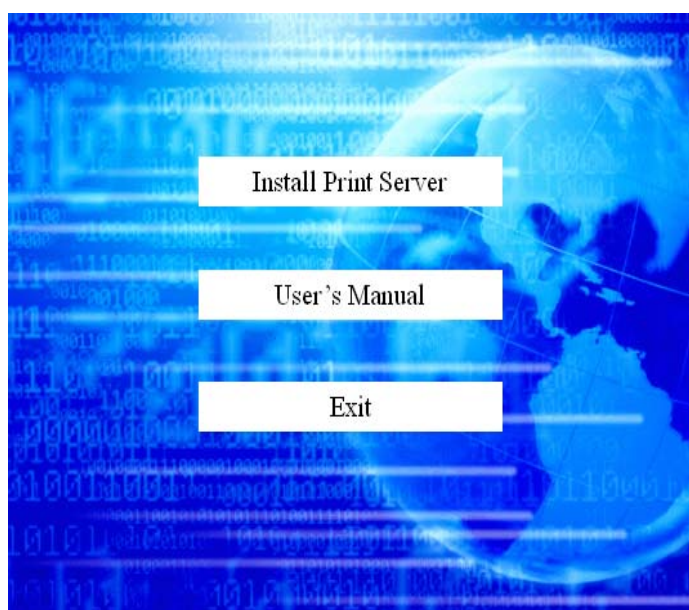
Tip: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

3.2 Install the Software into Your Computers

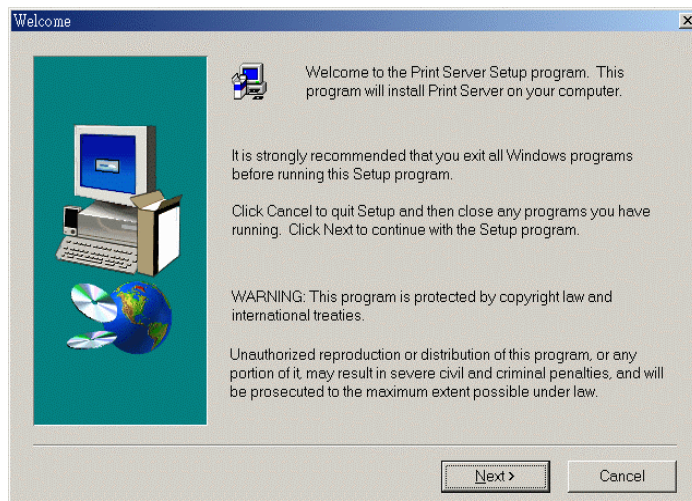
Skip this section if you do not want to use the print server function of this product.

Notice: If you are using Windows 2000/XP, please refer to **Chapter 5 Printer - 5.3 Configuring on Windows 2000 and XP Platforms**. It is not necessary to setup any program and the print-server can work.

Step 1: Insert the installation CD-ROM into the CD-ROM drive. The following window will be shown automatically. If it isn't, please run "install.exe" on the CD-ROM.

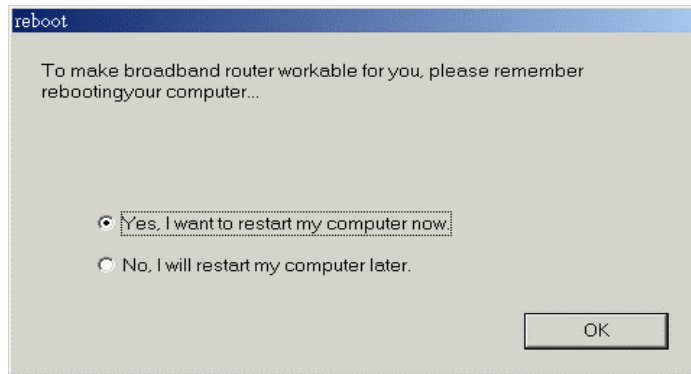


Step 2: Click on the **INSTALL** button. Wait until the following **Welcome** dialog to appear, and click on the **Next** button.



Step 3: Select the destination folder and click on the **Next** button. Then, the setup program will begin to install the programs into the destination folder .Step 4: When the following window is displayed, click on the **Finish** button.

Select the item to restart the computer and then click the **OK** button to reboot your computer.



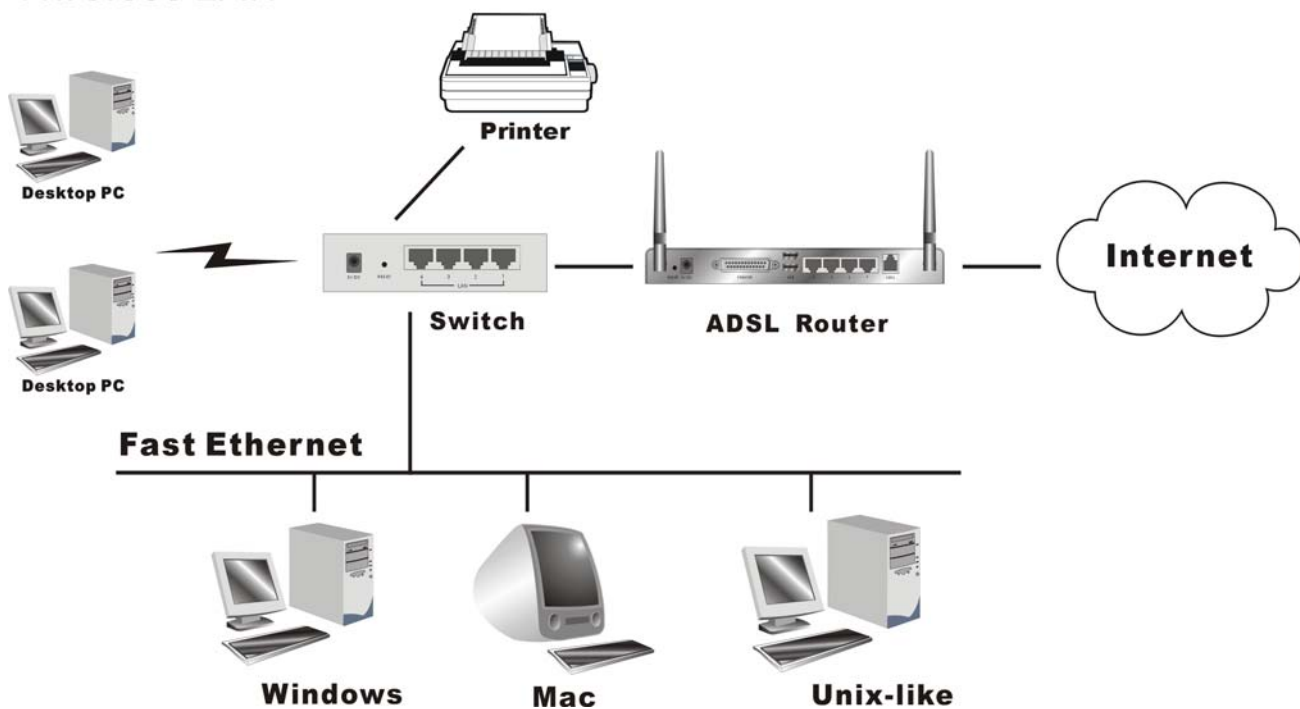
Step 4: After rebooting your computer, the software installation procedure is finished.

Now, you can configure the NAT Router (refer to Chapter 4) and setup the Print Server (refer to Chapter 5).

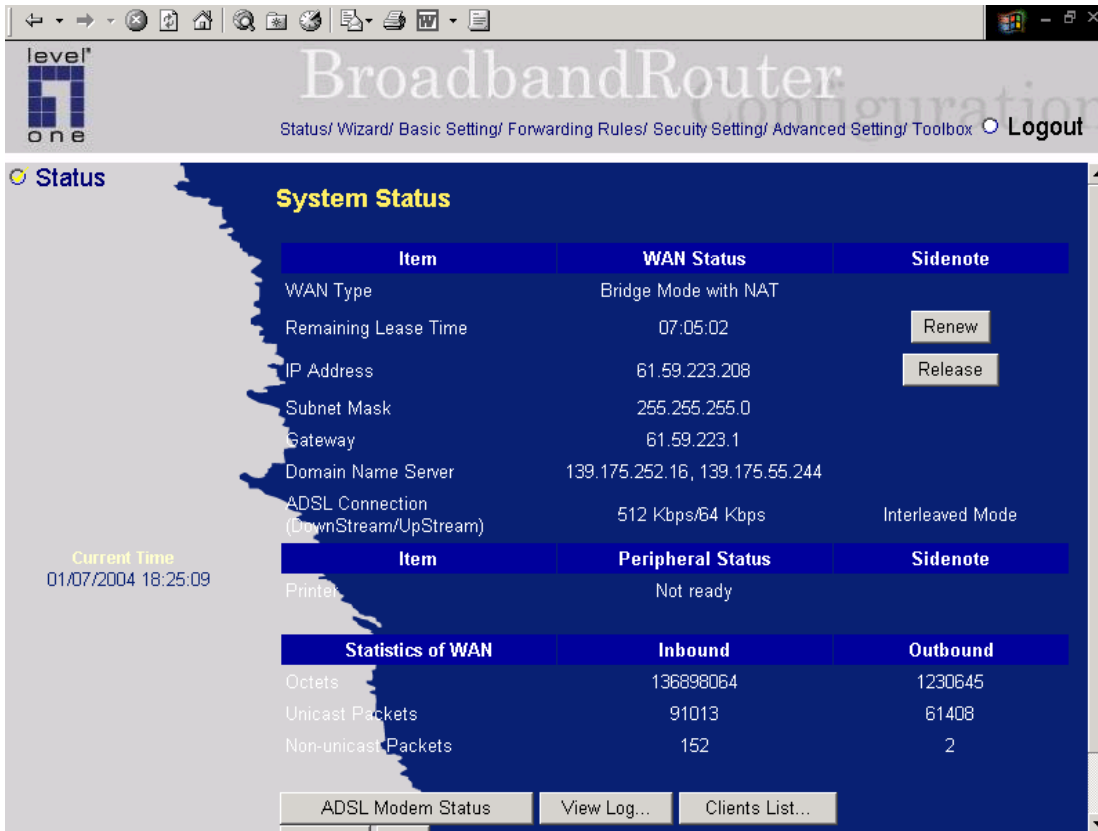
Chapter 4 Configuring ADSL Wireless Broadband Router

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.

Wireless LAN



4.1 Start-up and Log in



The screenshot shows the web interface of a BroadbandRouter. The browser window title is "BroadbandRouter" and the address bar shows "http://192.168.123.254". The interface has a dark blue background with white text. At the top, there is a navigation menu with options: Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox and a Logout button. The main content area is titled "System Status" and is divided into several sections:

- System Status Table:**

Item	WAN Status	Sidenote
WAN Type	Bridge Mode with NAT	
Remaining Lease Time	07:05:02	<input type="button" value="Renew"/>
IP Address	61.59.223.208	<input type="button" value="Release"/>
Subnet Mask	255.255.255.0	
Gateway	61.59.223.1	
Domain Name Server	139.175.252.16, 139.175.55.244	
ADSL Connection (DownStream/UpStream)	512 Kbps/64 Kbps	Interleaved Mode
- Peripheral Status Table:**

Item	Peripheral Status	Sidenote
Printer	Not ready	
- Statistics of WAN Table:**

Item	Inbound	Outbound
Octets	136898064	1230645
Unicast Packets	91013	61408
Non-unicast Packets	152	2

At the bottom of the System Status section, there are three buttons: "ADSL Modem Status", "View Log...", and "Clients List...". On the left side of the System Status section, there is a "Current Time" display showing "01/07/2004 18:25:09".

Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: **http://192.168.123.254**.

After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter the system password (the factory setting is "admin") in the **System Password** field and click on the **Log in** button. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.

4.2 Status

The screenshot shows the 'BroadbandRouter Configuration' web interface. The 'Status' section is active, displaying the following information:

System Status

Item	WAN Status	Sidenote
WAN Type	Bridge Mode with NAT	
Remaining Lease Time	07:05:43	
IP Address	61.59.223.208	
Subnet Mask	255.255.255.0	
Gateway	61.59.223.1	
Domain Name Server	139.175.252.16, 139.175.55.244	
ADSL Connection (DownStream/UpStream)	512 Kbps/64 Kbps	Interleaved Mode

Current Time: 01/07/2004 18:25:34

Item	Peripheral Status	Sidenote
Printer	Not ready	

Statistics of WAN

	Inbound	Outbound
Octets	135200672	1215045
Unicast Packets	89885	60628
Non-unicast Packets	152	2

Buttons: Refresh, Help. System Time: 01/07/2004 18:24:31

This option provides the function for observing this product's working status:

A. WAN Port Status.

If the WAN port is assigned a dynamic IP, there may appear a **“Renew”** or **“Release”** button on the Sidenote column. You can click this button to renew or release IP manually.

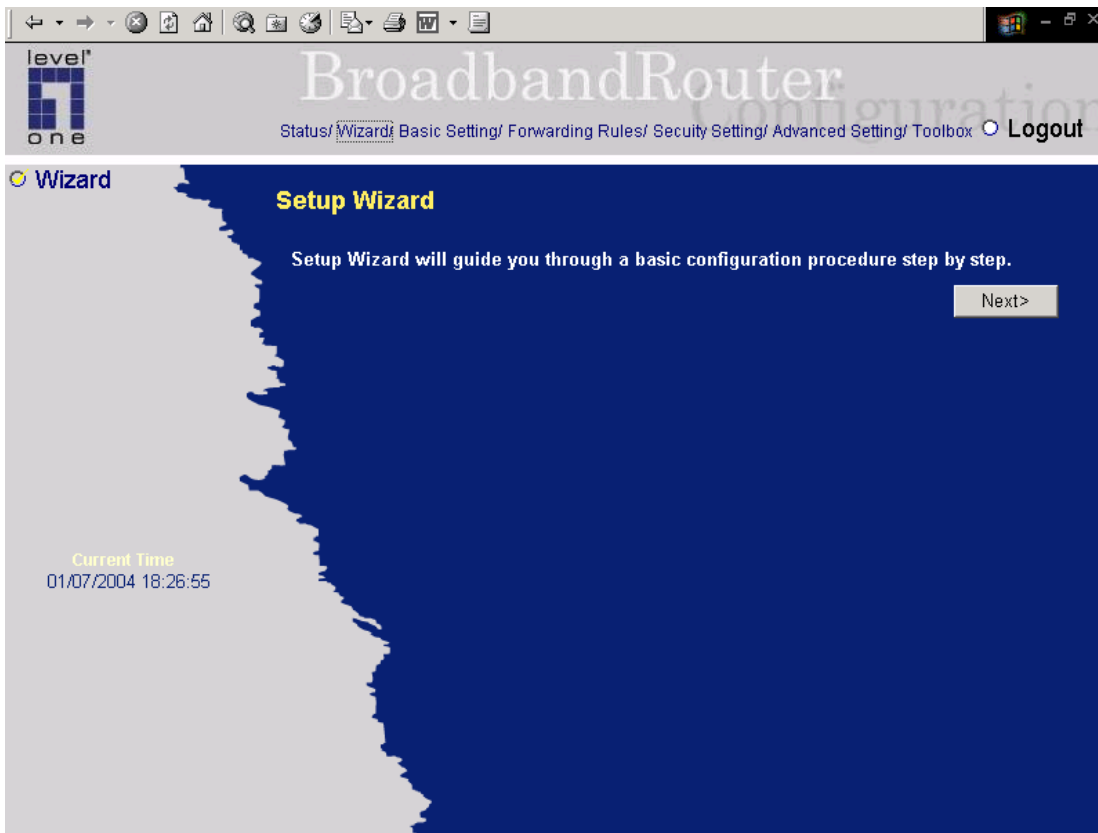
B. Printer Status. The possible kinds of printer status include *“Ready”*, *“Not ready”*, *“Printing...”*, and *“Device error”*.

When a job is printing, there may appear a “Kill Job” button on the Sidenote column. You can click this button to kill current printing job manually.

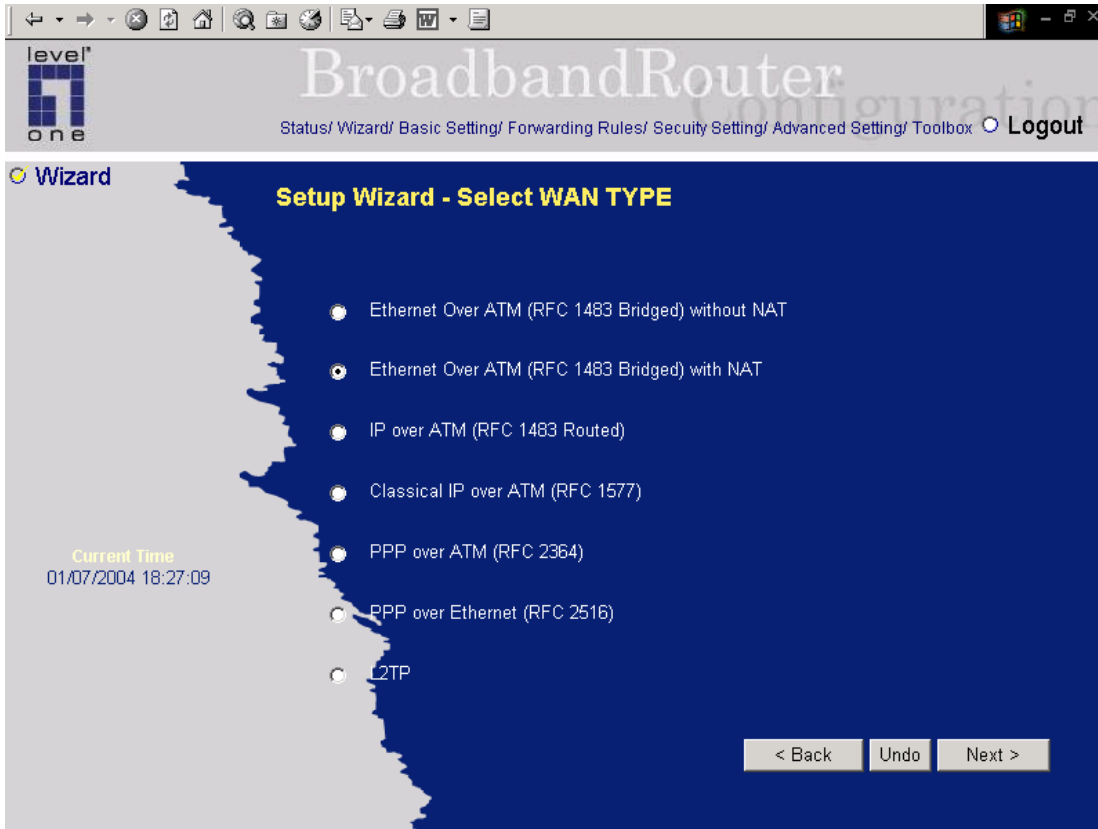
C. Statistics of WAN: enables you to monitor inbound and outbound packets

Notice: For the WBR-3402B, it can support both Annex B and U-R2 ADSL line coding schemes. The default setting is Annex B. If your ISP used U-R2 scheme, you have to change the line coding scheme to U-R2, and then reboot this product to successfully establish the connection with ISP

4.3 Wizard

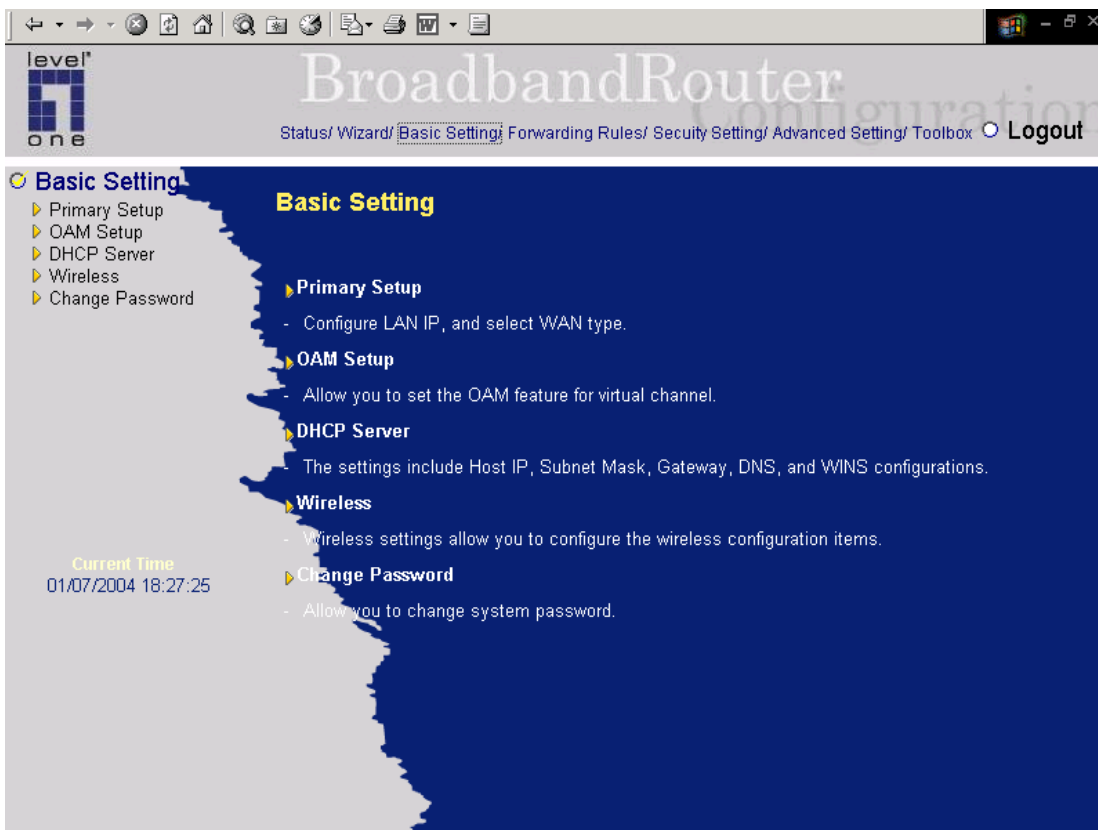


Setup Wizard will guide you through a basic configuration procedure step by step. Press "Next >"



Setup Wizard - Select WAN Type: For detail settings, please refer to **4.4.1 primary setup**.

4.4 Basic Setting



4.4.1 Primary Setup – WAN Type

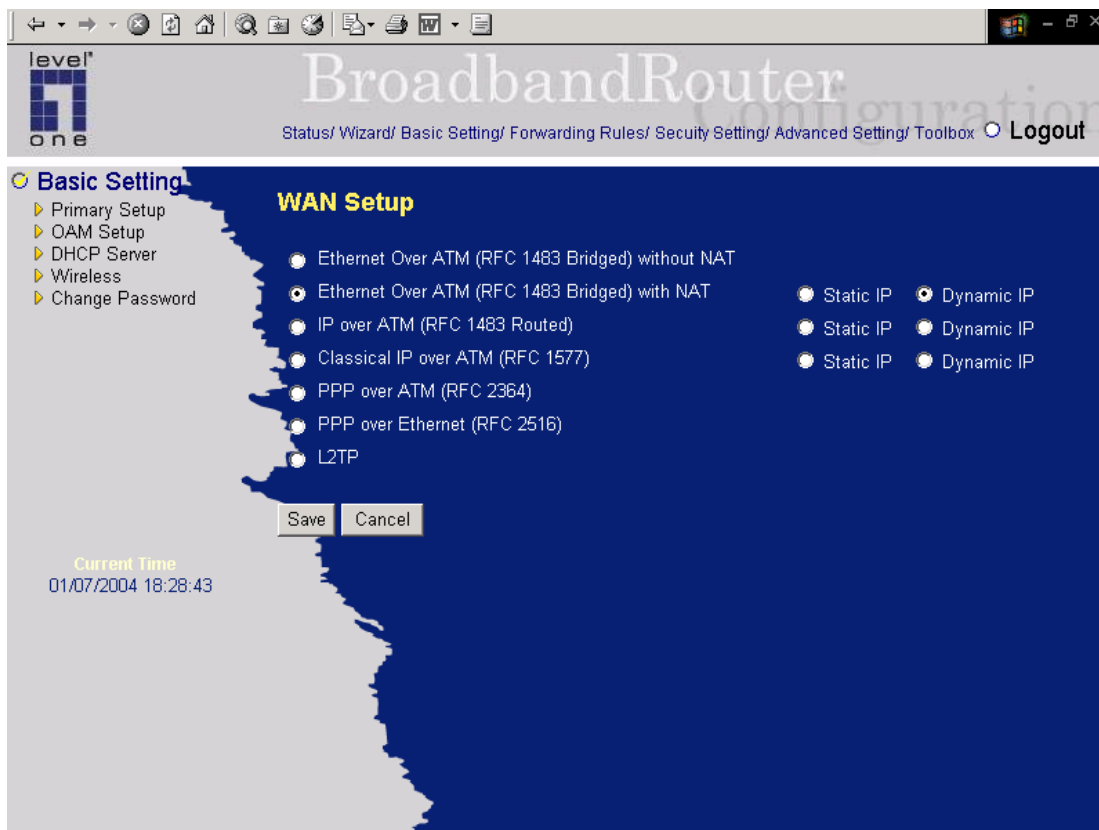
The screenshot shows the configuration interface for a level one BroadbandRouter. The page title is "BroadbandRouter Configuration" and the breadcrumb trail is "Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout". The "Basic Setting" menu is expanded to show "Primary Setup".

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	RFC1483 Bridge Mode with NAT Change...
WAN IP Mode	Dynamic IP Address
WAN's MAC Address	FF-FF-FF-FF-FF-FF Save Clone MAC
Renew IP Forever	<input checked="" type="checkbox"/> Enable (Auto-reconnect)
Data Encapsulation	LLC
VPI Number	0
VCI Number	33
Schedule type	UBR

Current Time: 01/07/2004 18:28:10

Buttons: [Save](#) [Undo](#) [Virtual Computer](#) [Help](#)

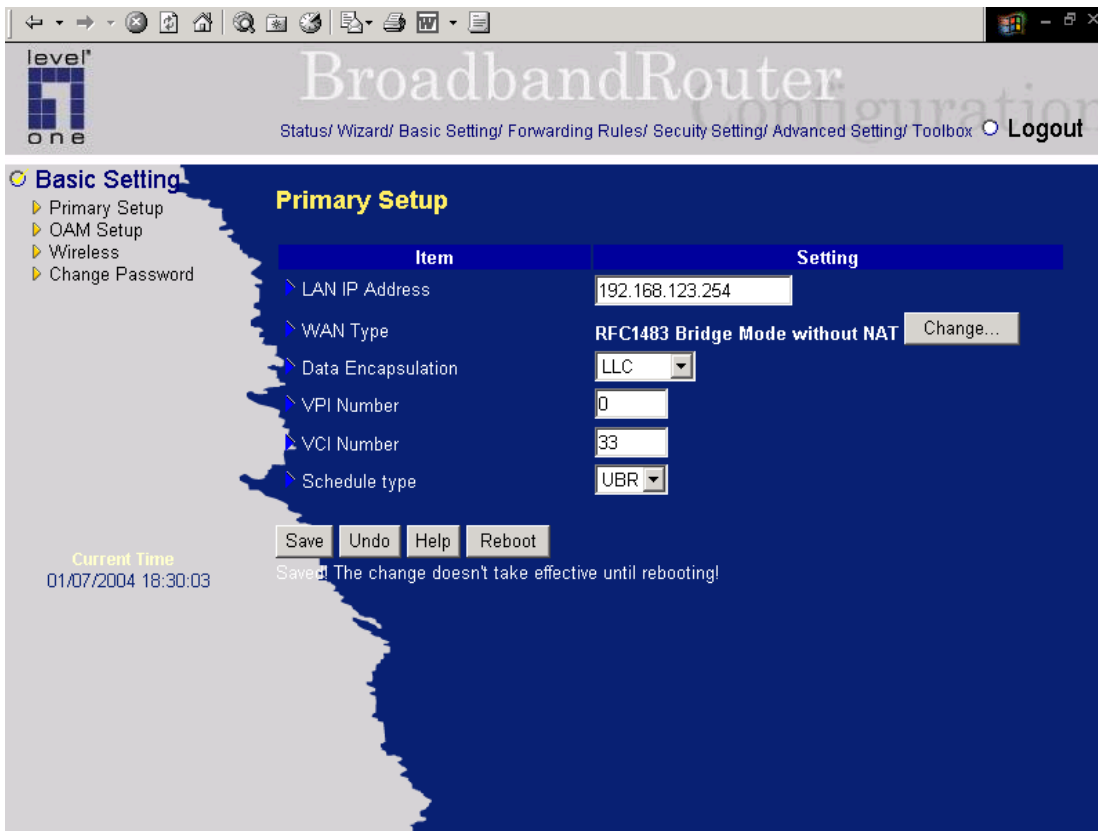
Press "Change"



This page is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following five options:
 - A. Ethernet Over ATM (RFC 1483 Bridged) without NAT
 - B. Ethernet Over ATM (RFC 1483 Bridged) with NAT
 - C. IP over ATM (RFC 1483 Routed).
 - D. Classical IP over ATM (RFC 1577).
 - E. PPP over ATM (RFC 2364).
 - F. PPP over Ethernet (RFC 2516).
3. **Data Encapsulation:** Two data encapsulation type are supported: LLC and vc-MUX. It is specified by your ISP. Once you finished above settings, click on the "Advanced Setting" button to another page for further configurations.

4.4.1.1 Ethernet Over ATM (RFC 1483 Bridged) without NAT



This WAN type disable the NAT, this device becomes a pure bridge between your LAN and WAN, all the clients in your LAN must have legal IPs. If you enable the NAT feature, you have to set the following WAN IP settings.

WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary/Secondary DNS

These settings are also specified by your ISP.

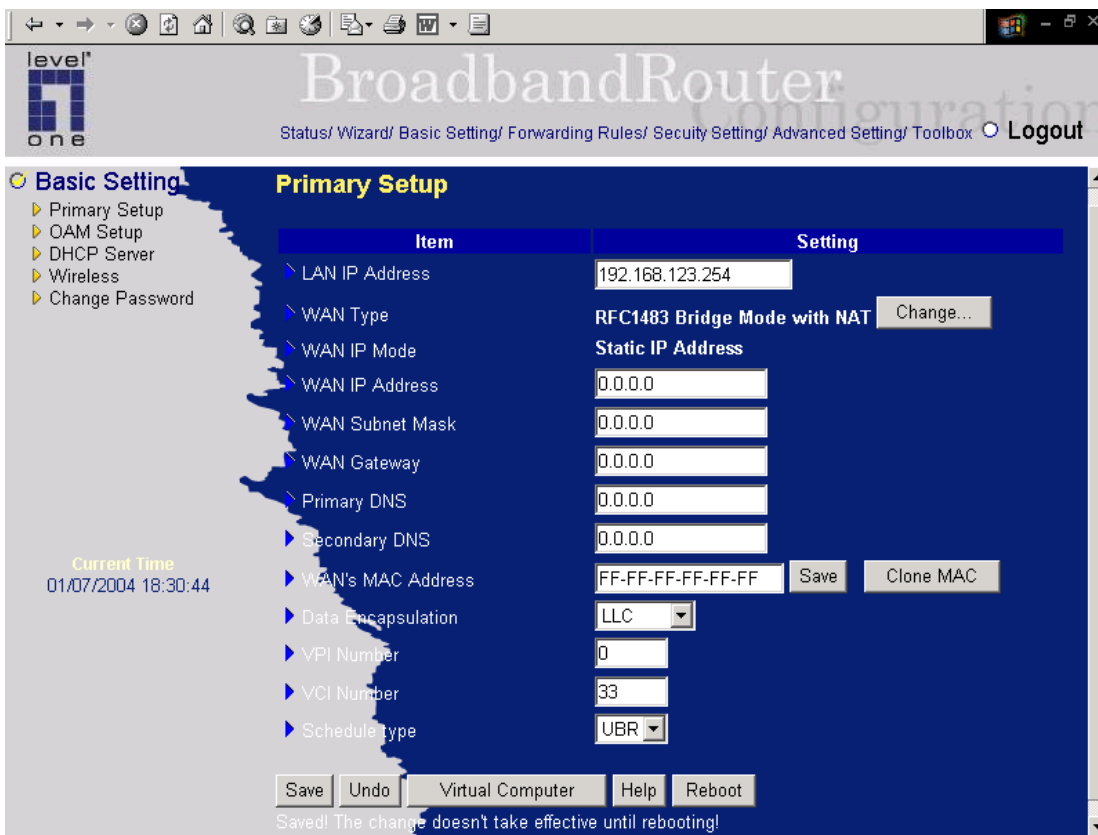
VPI/VCI Numbers:

The channel settings provided by your ISP.

Schedule Type:

The setting of the ADSL traffic schedule type. This device supports UBR (Un-specified bit rate) and CBR (Constant bit rate). Once you finished the required configuration, you must click on the "Save" button to save the configuration into Flash memory, and the reboot this device.

4.4.1.2 Ethernet Over ATM (RFC 1483 Bridged) with NAT



Dynamic IP Address: Obtain an IP address from ISP automatically.

Host Name: optional. Required by some ISPs, for example, @Home.

1. **Renew IP Forever:** this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

level one
BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox **Logout**

Basic Setting

- ▶ Primary Setup
- ▶ OAM Setup
- ▶ DHCP Server
- ▶ Wireless
- ▶ Change Password

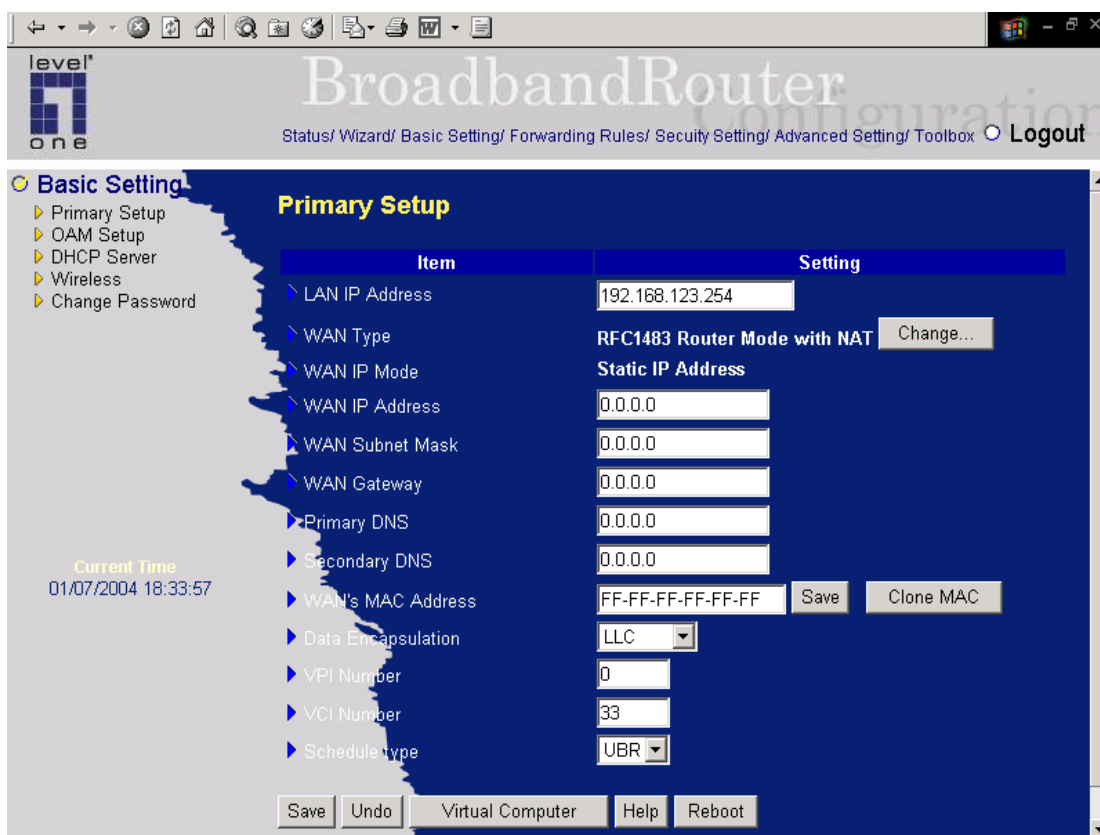
Primary Setup

Item	Setting
▶ LAN IP Address	192.168.123.254
▶ WAN Type	RFC1483 Bridge Mode with NAT <input type="button" value="Change..."/>
▶ WAN IP Mode	Dynamic IP Address
▶ WAN's MAC Address	FF-FF-FF-FF-FF-FF <input type="button" value="Save"/> <input type="button" value="Clone MAC"/>
▶ Renew IP Forever	<input checked="" type="checkbox"/> Enable (Auto-reconnect)
▶ Data Encapsulation	LLC
▶ VPI Number	0
▶ VCI Number	33
▶ Schedule type	UBR

Current Time
01/07/2004 18:38:47

Saved! The change doesn't take effective until rebooting!

4.4.1.3 IP over ATM (RFC 1483 Routed)



In the Router Mode, NAT is always enabled. You have to set the following WAN IP settings:

WAN IP Mode:

This product supports two WAN IP modes: static and dynamic. If you select dynamic mode, it will try to get a legal IP and WAN settings from ISP's DHCP server. If you select static mode, you have to set the following WAN setting manually.

WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary/Secondary DNS

These settings are assigned by your ISP.

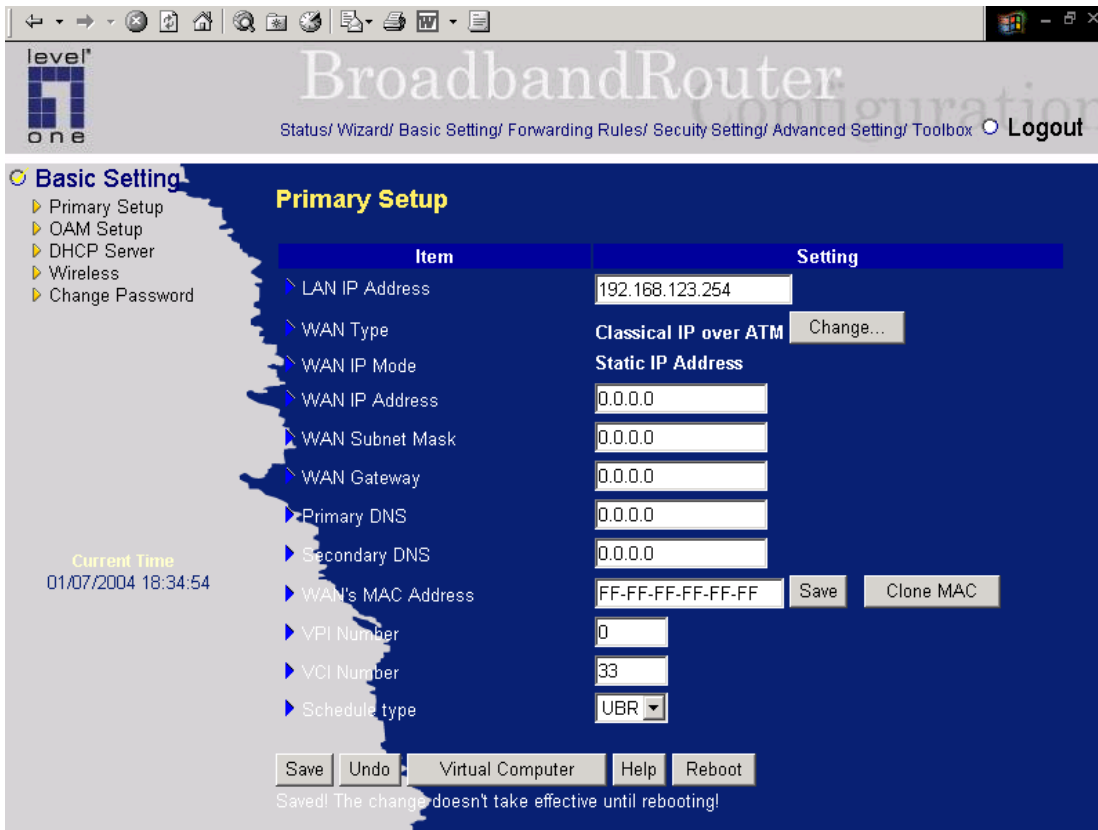
VPI/VCI Numbers:

The channel settings provided by your ISP.

Schedule Type:

The setting of the ADSL traffic schedule type. This device supports UBR (Un-specified bit rate) and CBR (Constant bit rate). Once you finished the required configuration, you must click on the "Save" button to save the configuration into Flash memory, and the reboot this device.

4.4.1.4 Classical IP over ATM (RFC 1577)



In the Classical IP over ATM Mode, NAT is always enabled. You have to set the following WAN IP settings:

WAN IP Mode:

This product supports two WAN IP modes: static and dynamic. If you select dynamic mode, it will try to get a legal IP and WAN settings from ISP's DHCP server. If you select static mode, you have to set the following WAN setting manually.

WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary/Secondary DNS

These settings are assigned by your ISP.

VPI/VCI Numbers:

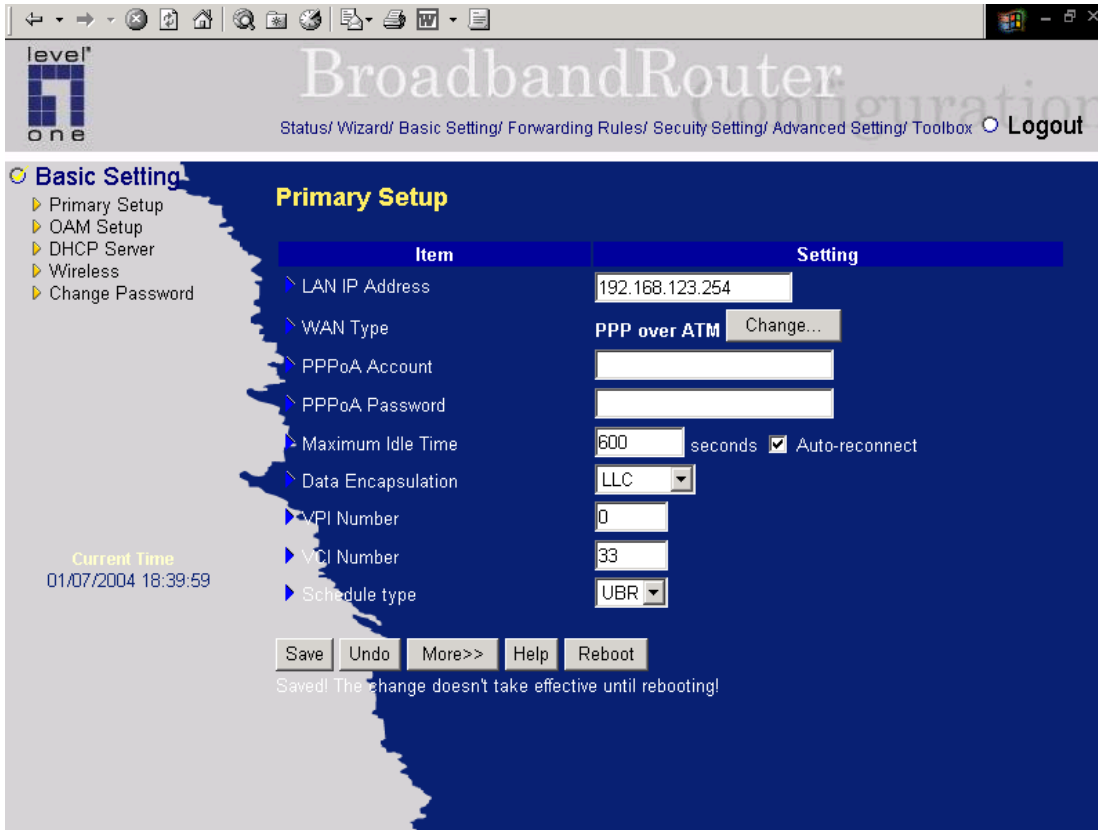
The channel settings provided by your ISP.

Schedule Type:

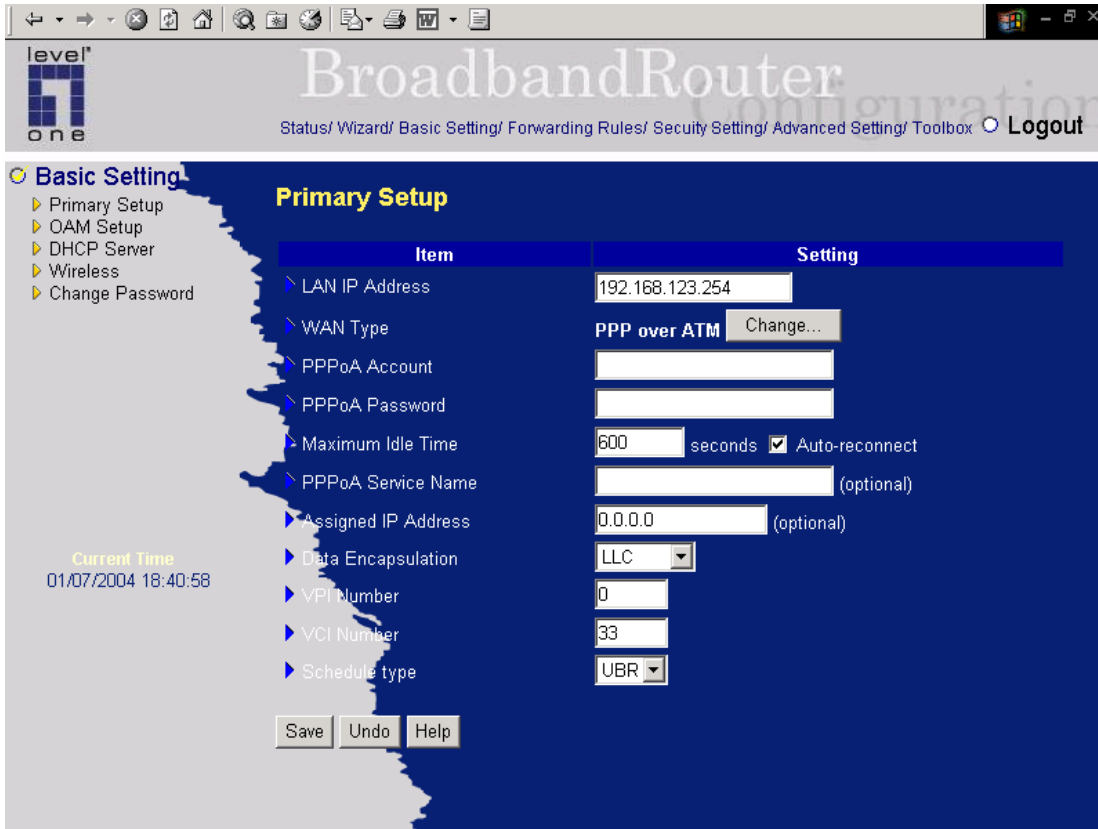
The setting of the ADSL traffic schedule type. This device supports UBR (Un-specified bit rate) and CBR (Constant bit rate). Once you finished the required configuration, you must click on the "Save"

button to save the configuration into Flash memory, and the reboot this device.

4.4.1.5 PPP over ATM (RFC 2364)



Press "More >>"



PPPoA Account/Password:

The account ID & password provided by your ISP.

Maximum Idle Time:

The time of no activity disconnect to your PPPoA session. You can also set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will automatically connect to ISP after system is restarted or connection is dropped.

VPI/VCI Numbers:

The channel settings provided by your ISP.

Schedule Type:

The setting of the ADSL traffic schedule type. This device supports UBR (Un-specified bit rate) and CBR (Constant bit rate).

PPPoA Service Name:

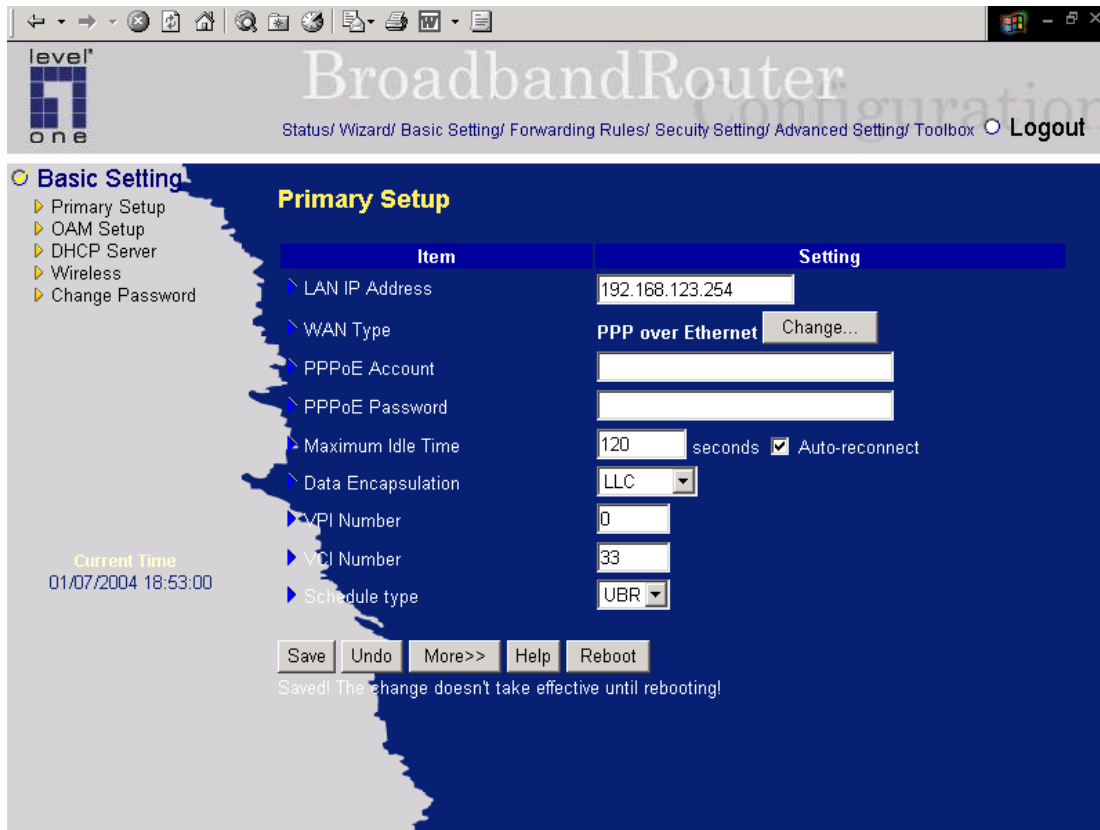
Optional. Input the service name if your ISP requires it.

Assigned IP Address:

Optional. Required by some ISPs. Once you finished the required configuration, you must click on the

"Save" button to save the configuration into Flash memory, and the reboot this device.

4.4.1.6 PPP over Ethernet (RFC 2516)



PPPoE Account/Password:

The account ID & password provided by your ISP.

Maximum Idle Time:

The time of no activity disconnect to your PPPoE session. You can also set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will automatically connect to ISP after system is restarted or connection is dropped.

VPI/VCI Numbers:

The channel settings provided by your ISP.

Schedule Type:

The setting of the ADSL traffic schedule type. This device supports UBR (Un-specified bit rate) and CBR (Constant bit rate).

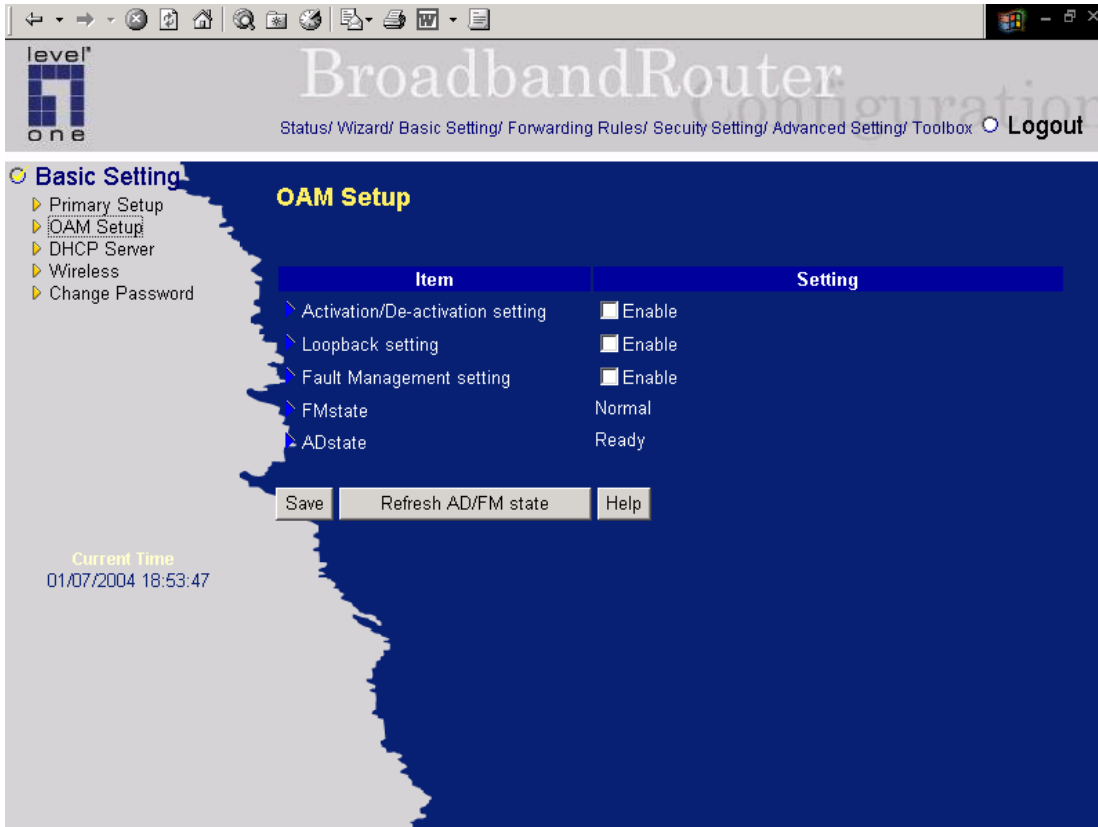
PPPoE Service Name:

Optional. Input the service name if your ISP requires it.

Assigned IP Address:

Optional. Required by some ISPs. Once you finished the required configuration, you must click on the "Save" button to save the configuration into Flash memory, and the reboot this device.

4.4.2 OAM Server



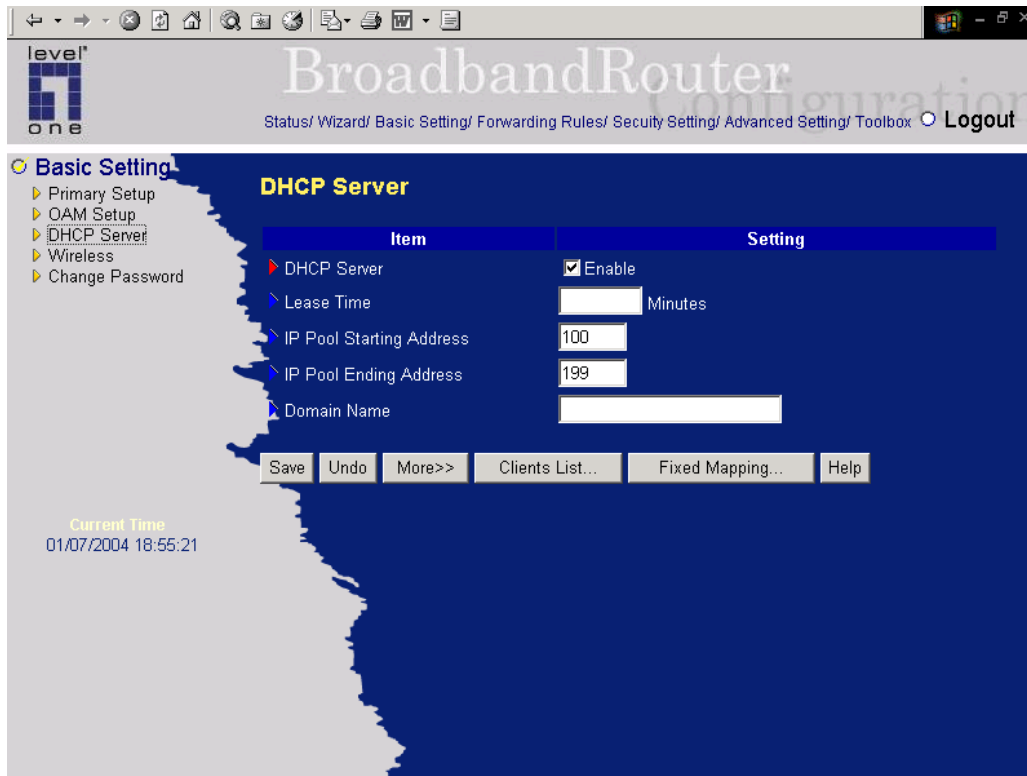
In this page, you can set the OAM feature for virtual channel.

First click on the Enable or Disable circle for the settings of OAM Function, Activation/De-activation, Loopback, and Fault Management individually.

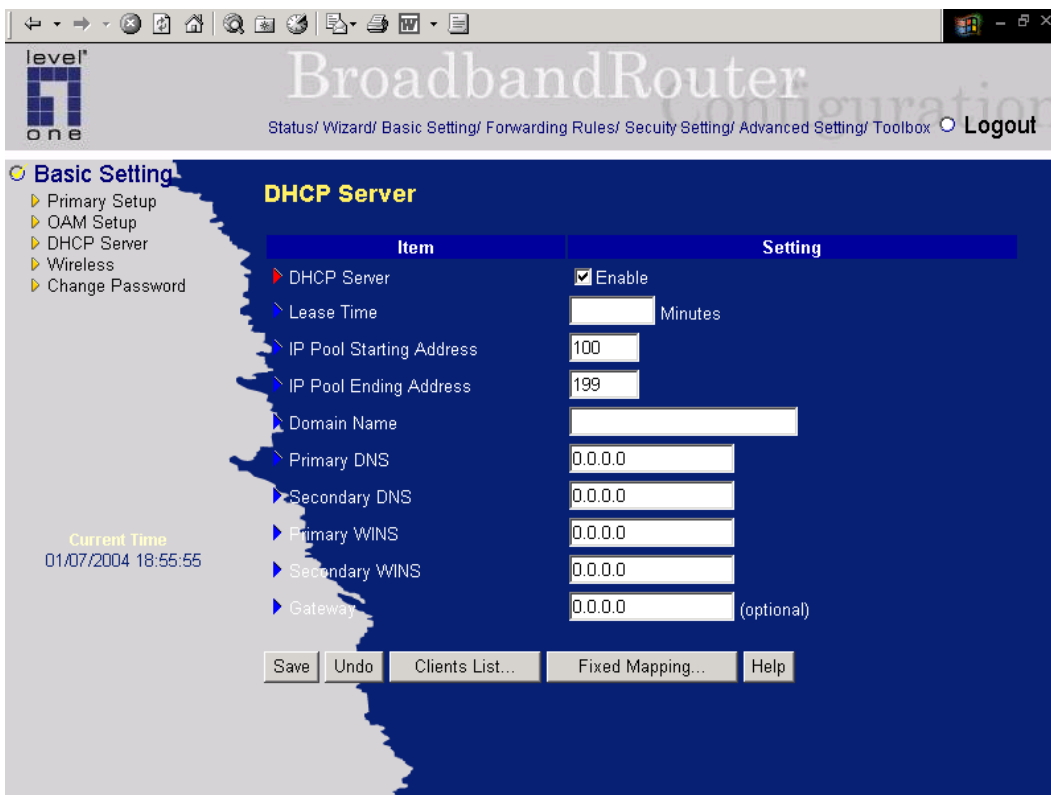
Then, click on the "Save" button to finish the configuration of the selected session.

Once you set the appropriate OAM settings on virtual channel, you can see the corresponding up-to-date maintenance status by clicking the "Refresh AD/FM State" button in this page.

4.4.3 DHCP Server



Press "More"

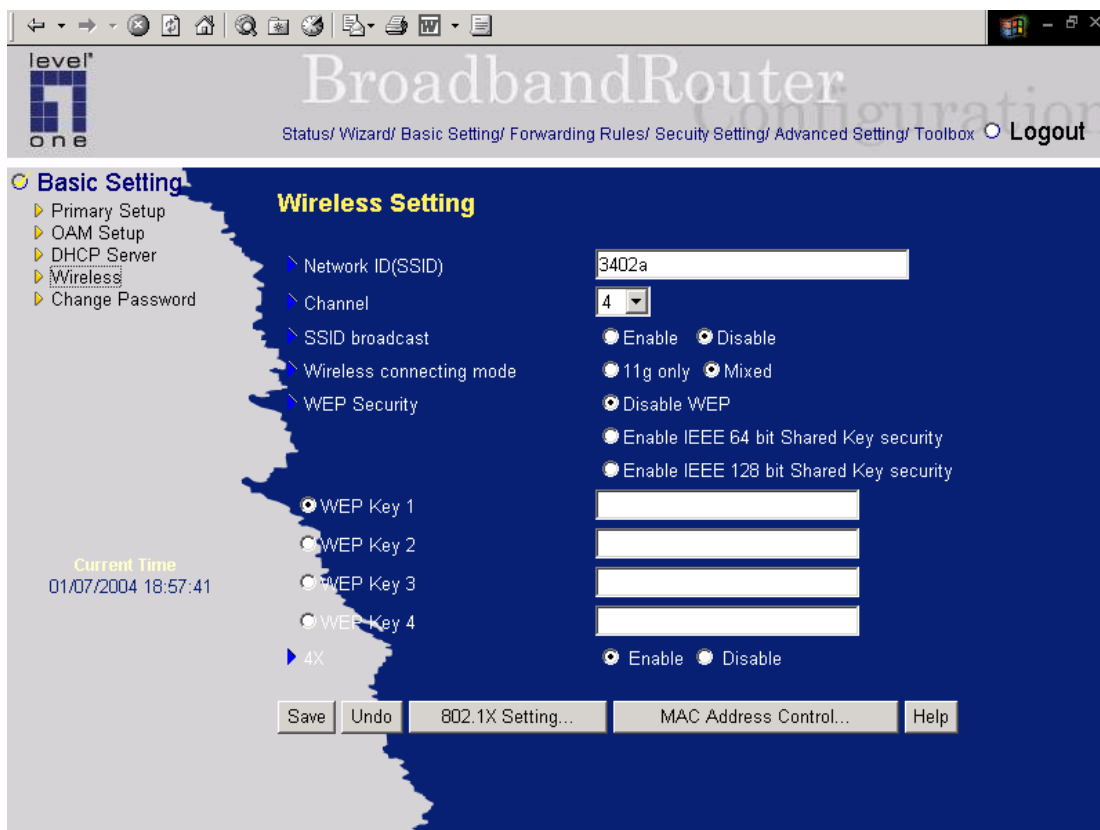


The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations.

It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

1. **DHCP Server:** Choose "Disable" or "Enable."
2. **Lease Time:** this feature allows you to configure IP's lease time (DHCP client).
3. **IP pool starting Address/ IP pool starting Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name:** Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
7. **Gateway:** The Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

4.4.4 Wireless Setting, and 802.1X setting



Wireless settings allow you to set the wireless configuration items.

1. **Network ID(SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “**default**”)
2. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is as follow: **channel 6** for North America; **channel 7** for European (ETSI); **channel 7** for Japan.
3. **SSID Broadcast:** Enable or disable SSID via this option.
4. **Wireless Connecting Mode:** Choose your Connecting Mode. Mixed Mode allows 11Mbps or 54Mbps wireless adapter connection. 11g only mode only allows the connection from 54Mbps wireless adapter and will refuse the connection from 11 Mbps wireless adapter.
5. **WEP Security:** Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. The standardized IEEE 802.11 WEP (128 or 64-bit) is used here.
6. **WEP Key 1, 2, 3 & 4:** When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.
7. **Pass-phrase Generator:** Since hexadecimal characters are not easily remembered, this device offers a conversion utility to convert a simple word or phrase into hex.

6. **802.1X Setting**

802.1X

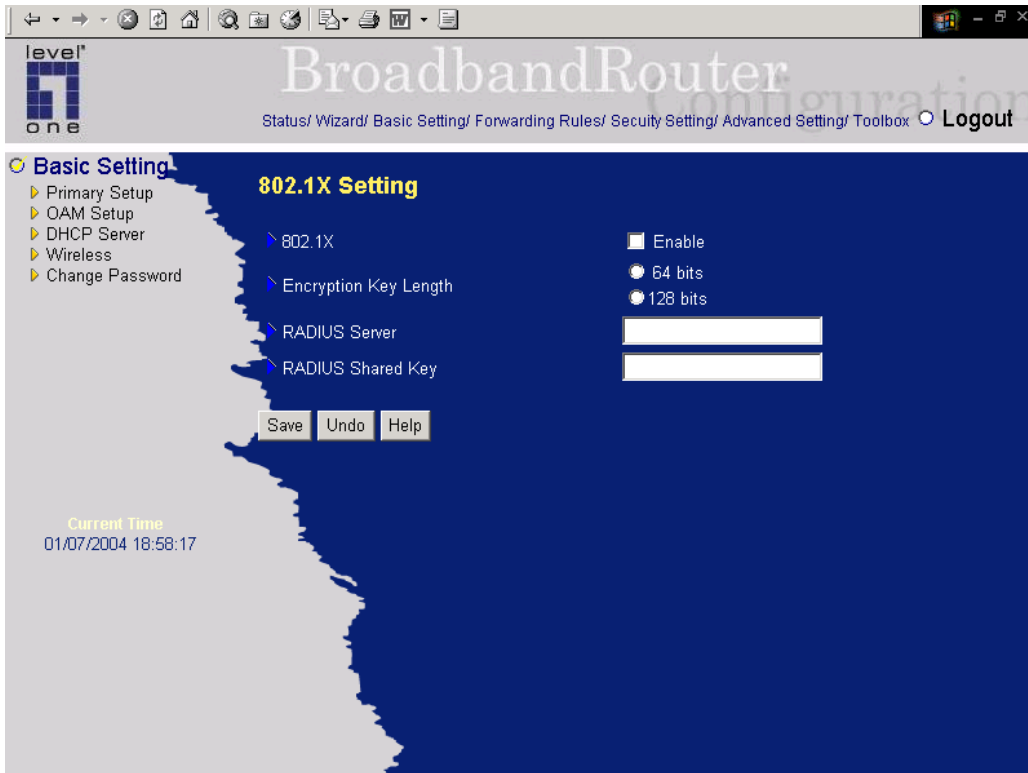
CheckBox was used to switch the function of the 802.1X. When the 802.1X function is enable, the Wireless user must **authenticate** to this router first to use the Network service.

RADIUS Server

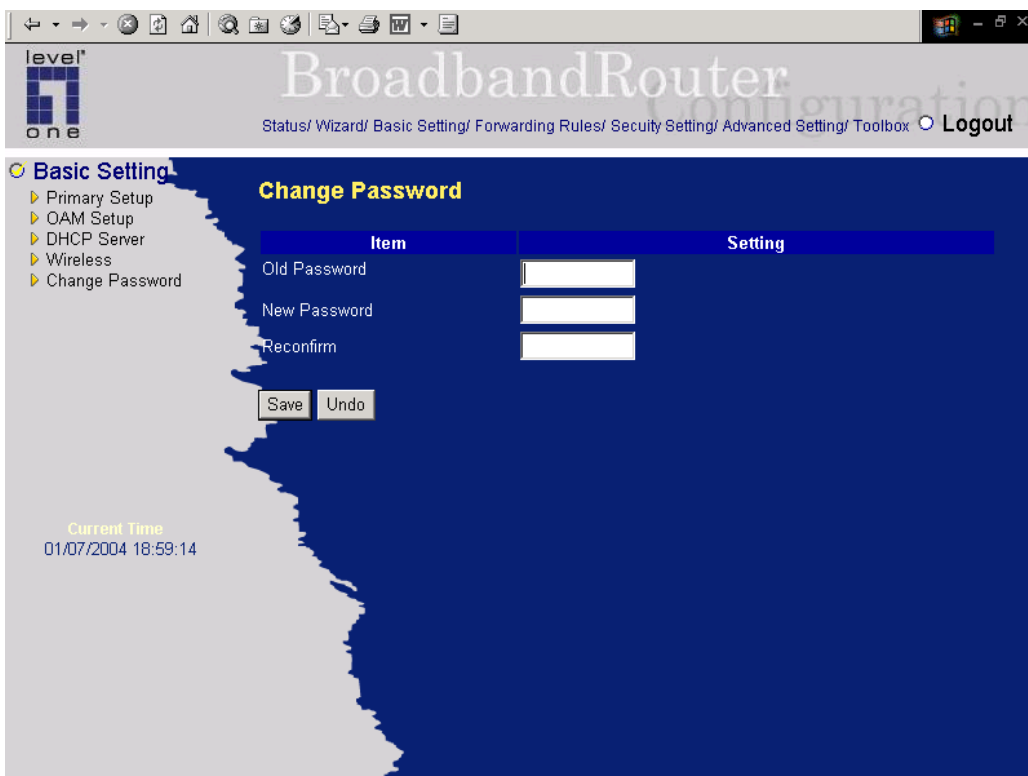
IP address or the 802.1X server’s domain-name.

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



4.4.5 Change Password



You can change Password here. We **strongly** recommend you to change the system password for security reason.

4.5 Forwarding Rules

The screenshot shows the 'Forwarding Rules' configuration page in the BroadbandRouter web interface. The breadcrumb navigation is: Status/ Wizard/ Basic Setting/ **Forwarding Rules**/ Security Setting/ Advanced Setting/ Toolbox Logout. The left sidebar shows 'Forwarding Rules' expanded with sub-items: Virtual Server, Special AP, and Miscellaneous. The main content area is titled 'Forwarding Rules' and contains the following sections:

- Virtual Server**: Allows others to access WWW, FTP, and other services on your LAN.
- Special Application**: This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous**:
 - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
 - Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).
 - UPnP Setting: UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals.

Current Time: 01/07/2004 18:59:47

4.5.1 Virtual Server

The screenshot shows the 'Virtual Server' configuration page in the BroadbandRouter web interface. The breadcrumb navigation is: Status/ Wizard/ Basic Setting/ Forwarding Rules/ **Virtual Server**/ Security Setting/ Advanced Setting/ Toolbox Logout. The left sidebar shows 'Forwarding Rules' expanded with sub-items: Virtual Server, Special AP, and Miscellaneous. The main content area is titled 'Virtual Server' and contains a table with 12 rows for configuring virtual servers.

ID	Service Ports	Server IP	Enable	Use Rule#
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
5	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
6	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
7	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
8	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
9	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
10	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
11	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
12	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="text"/>

Well known services: Copy to ID:

Schedule rule:

Current Time: 01/07/2004 18:59:57

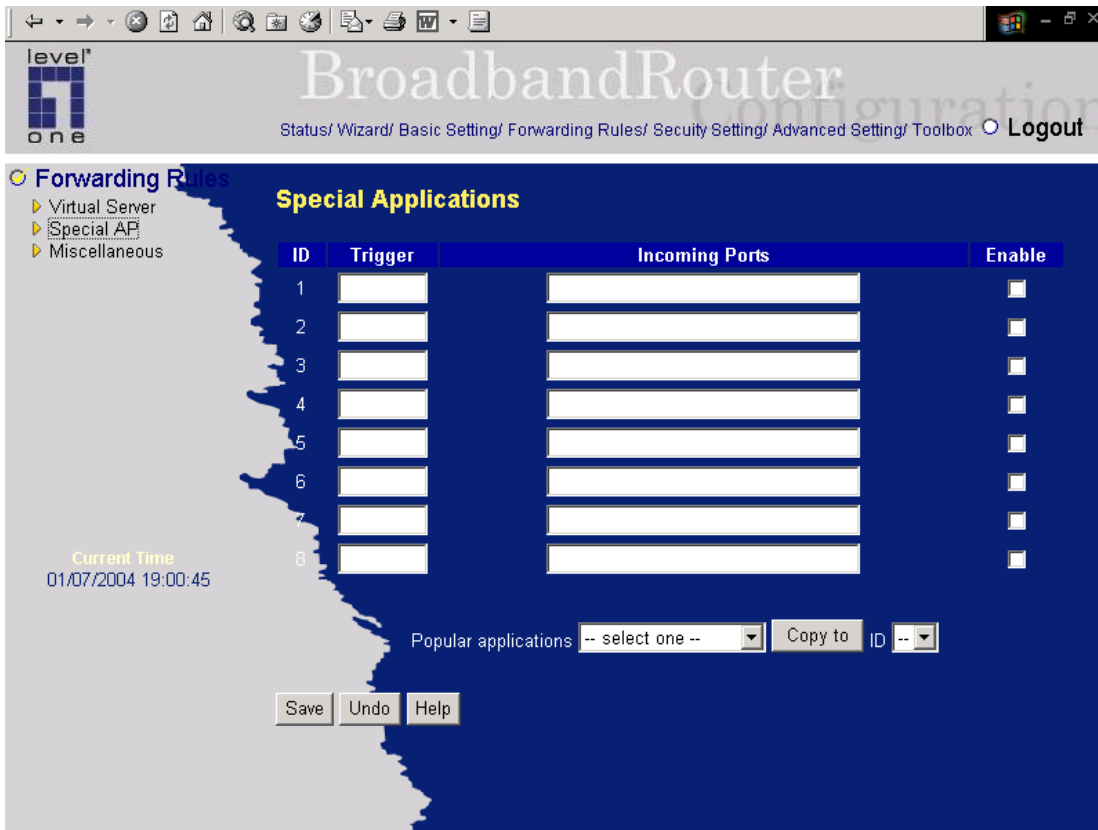
This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

4.5.2 Special AP



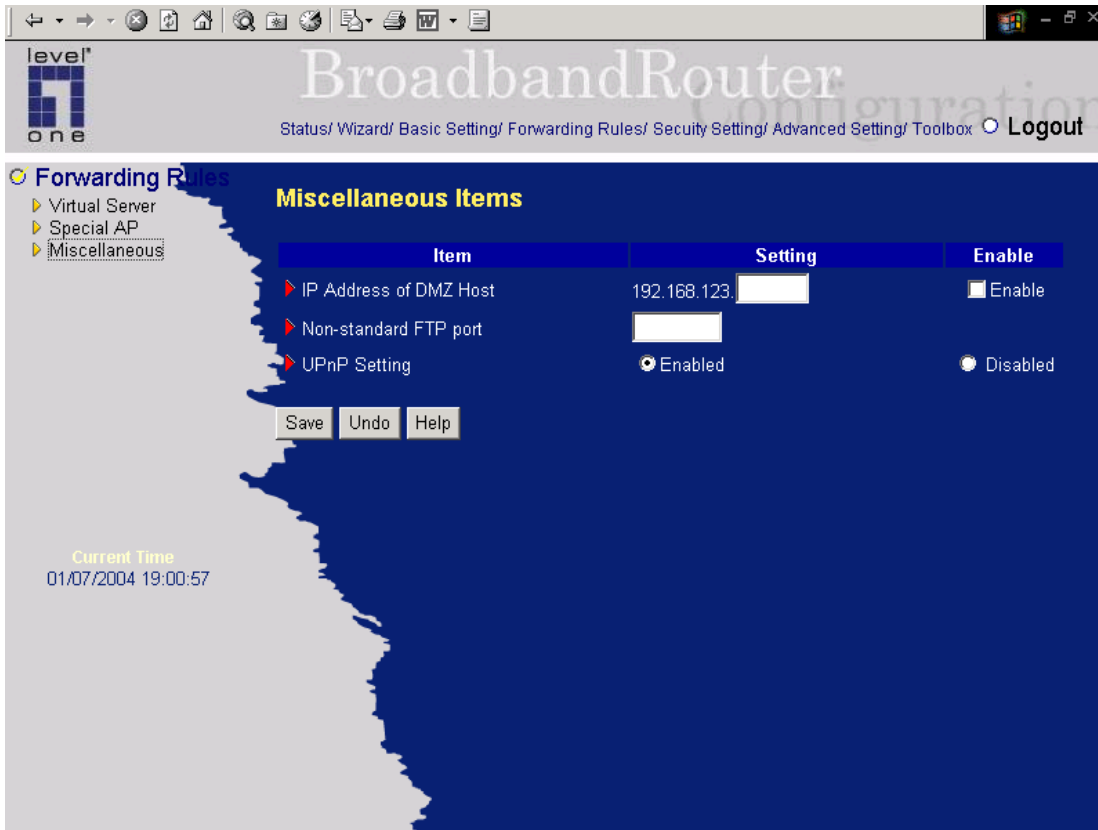
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

1. **Trigger:** the outbound port number issued by the application..
2. **Incoming Ports:** when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings. Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

4.5.3 Miscellaneous Items



IP Address of DMZ Host

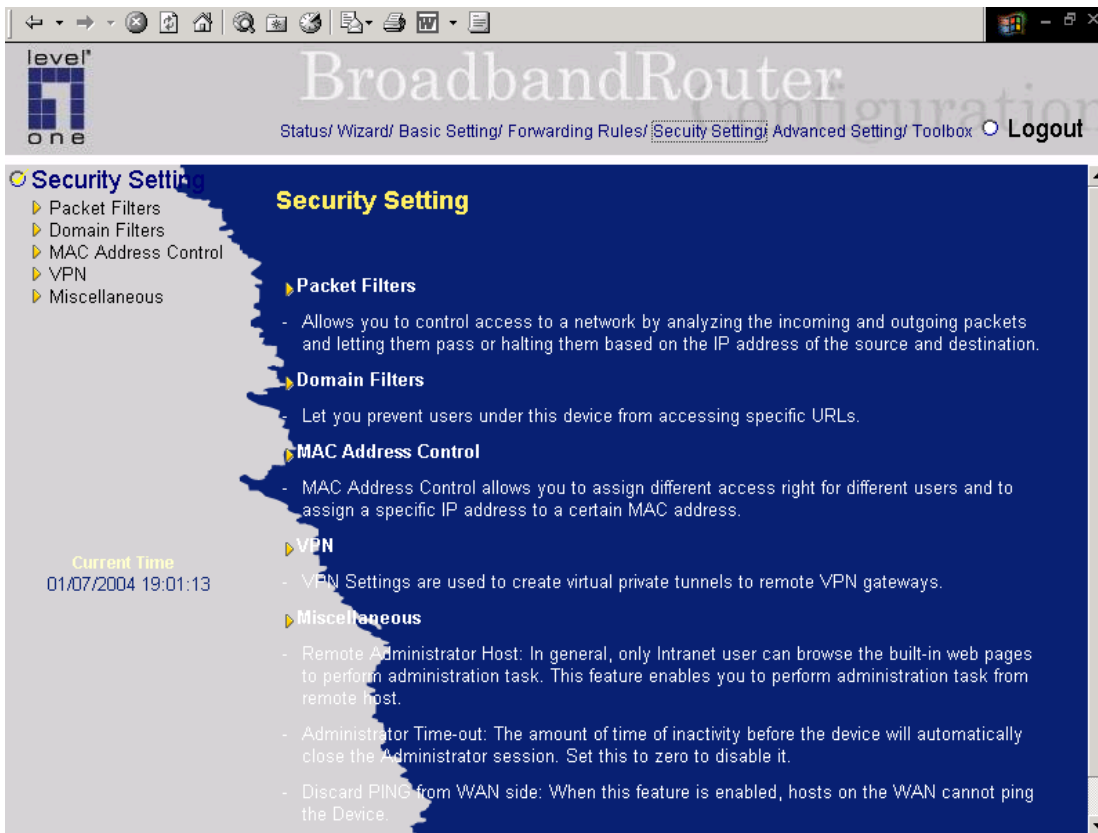
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

4.6 Security Settings

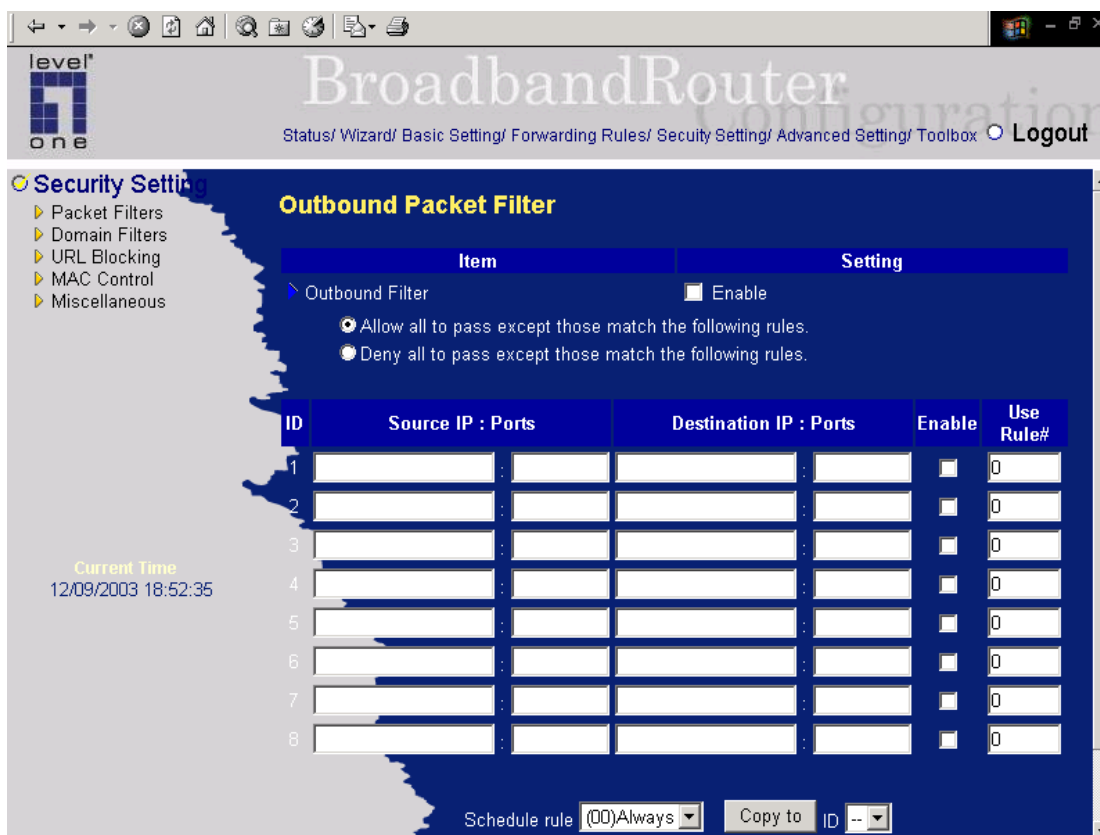


The screenshot displays the configuration interface for a LevelOne BroadbandRouter. The browser window title is "BroadbandRouter Configuration". The navigation menu includes: Status/ Wizard/ Basic Setting/ Forwarding Rules/ **Security Setting**/ Advanced Setting/ Toolbox Logout. The "Security Setting" section is expanded, showing a sidebar with sub-items: Packet Filters, Domain Filters, MAC Address Control, VPN, and Miscellaneous. The main content area lists the following security features:

- Packet Filters**
 - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters**
 - Let you prevent users under this device from accessing specific URLs.
- MAC Address Control**
 - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- VPN**
 - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- Miscellaneous**
 - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
 - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
 - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

Current Time: 01/07/2004 19:01:13

4.6.1 Packet Filter



Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. **Packet Filter** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

Each rule can be enabled or disabled individually.

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	100-192.168.123.149		<input checked="" type="checkbox"/>	0
2	23.10-192.168.123.20		<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

(192.168.123.100-192.168.123.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)

(192.168.123.10-192.168.123.20) They can do everything (block nothing)

Others are all blocked.

Example 2:

Inbound Packet Filter

Item	Setting
Inbound Filter	<input checked="" type="checkbox"/> Enable
	<input type="radio"/> Allow all to pass except those match the following rules.
	<input type="radio"/> Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	.100-192.168.123.119		<input checked="" type="checkbox"/>	0
2	.100-192.168.123.119		<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

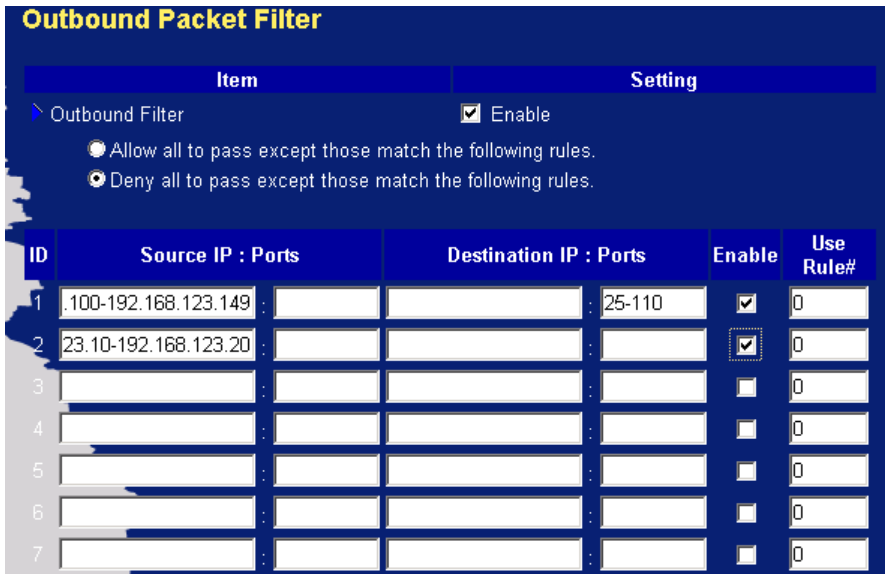
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

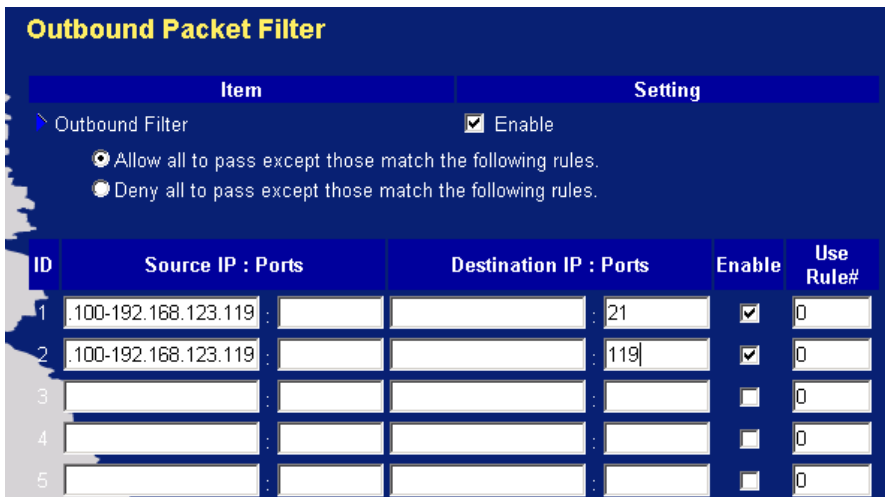
Example 1:



(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)
Others are all blocked.

Example 2:

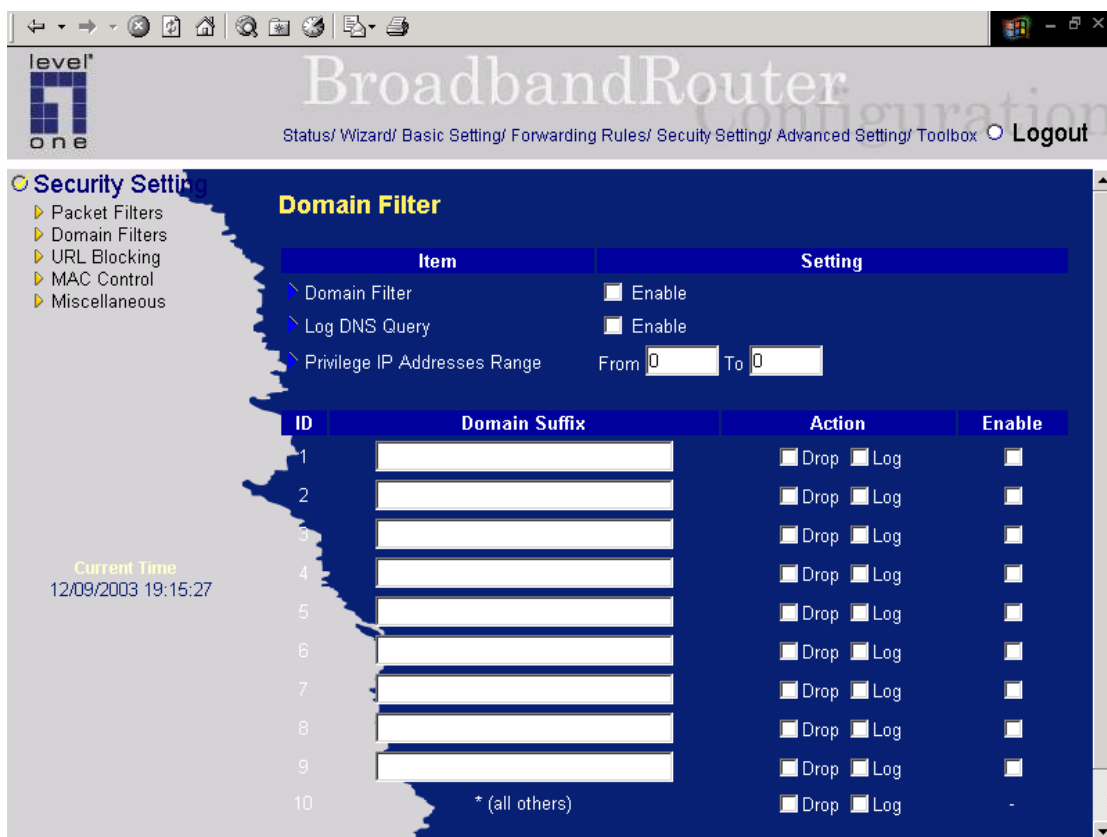


(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After **Outbound Packet Filter** setting is configured, click the **save** button.

4.6.2 Domain Filter



Domain Filter

let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

Action

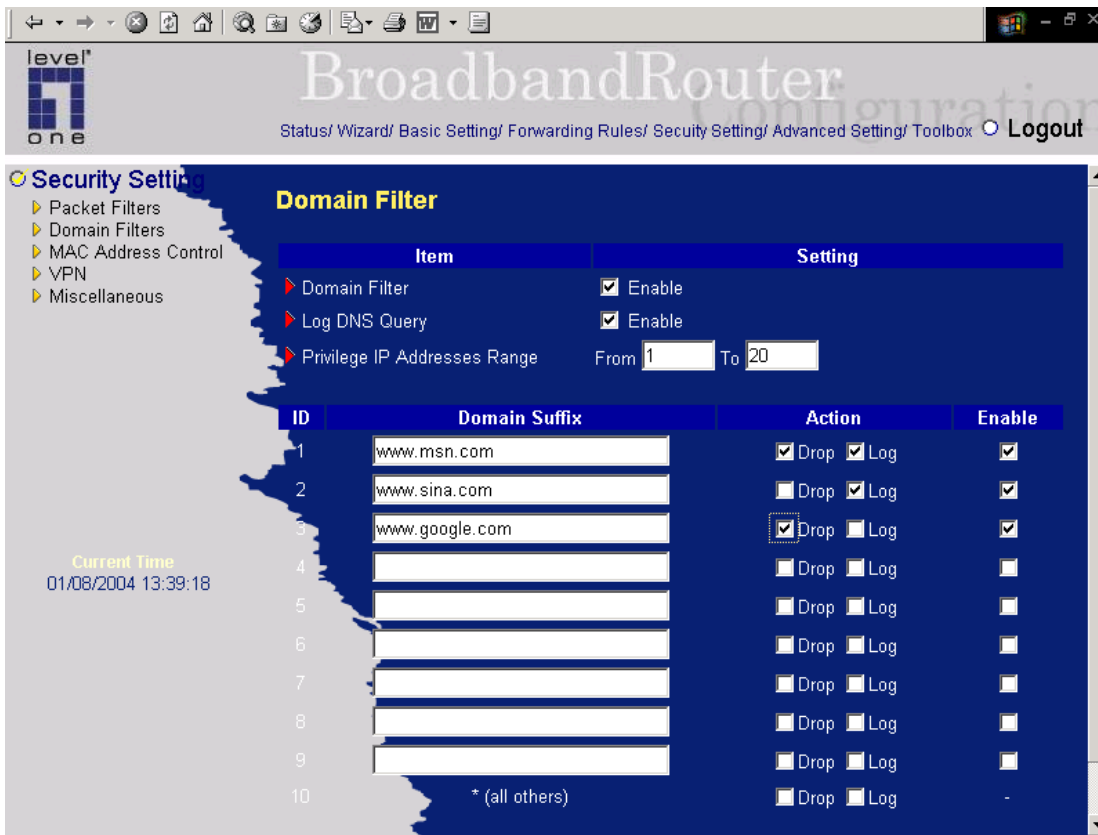
When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check drop to block the access. Check log to log these access.

Enable

Check to enable each rule.

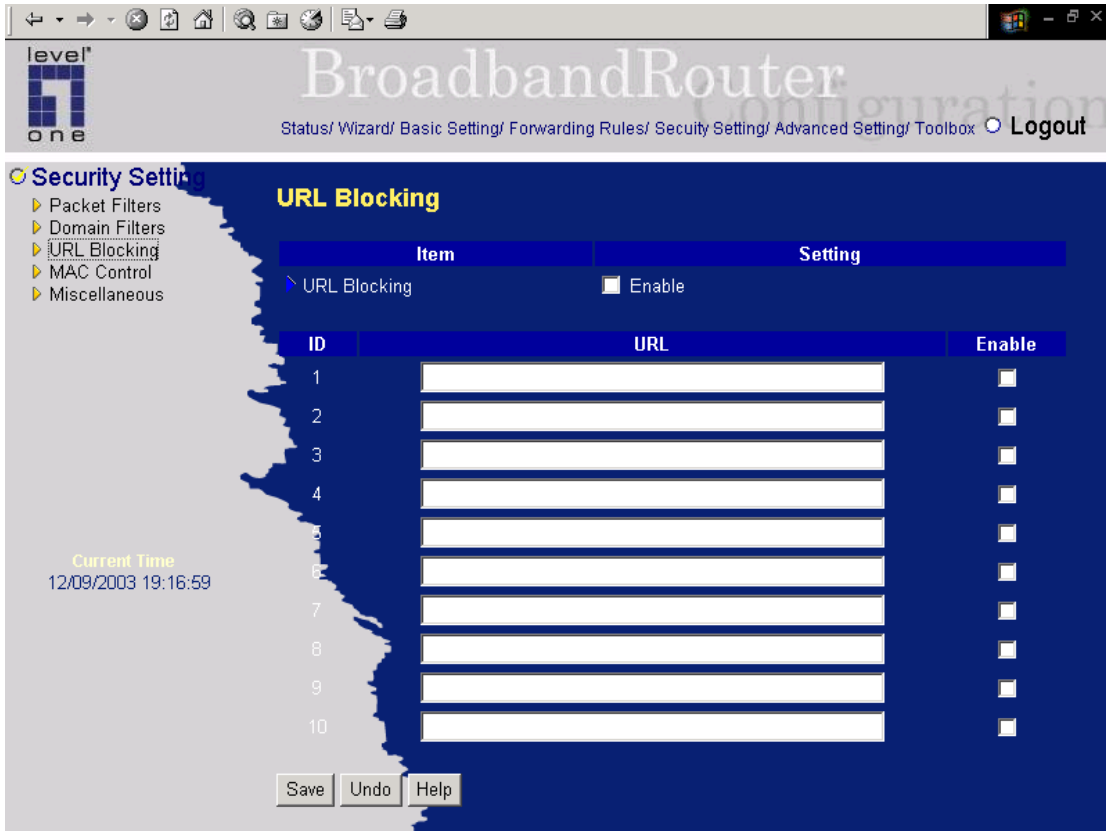
Example:



In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.
2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.
3. URL include "www.google.com" will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

4.6.3 URL Blocking



URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

URL Blocking Enable

Checked if you want to enable URL Blocking.

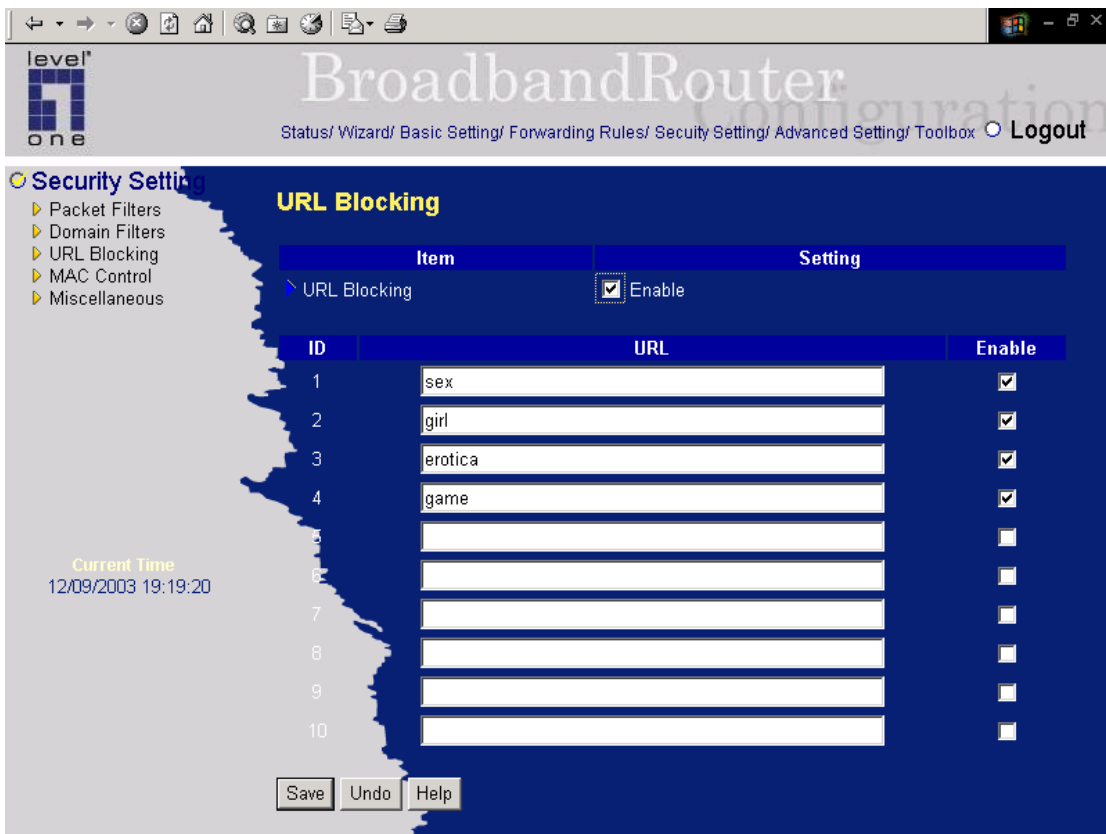
URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

Enable

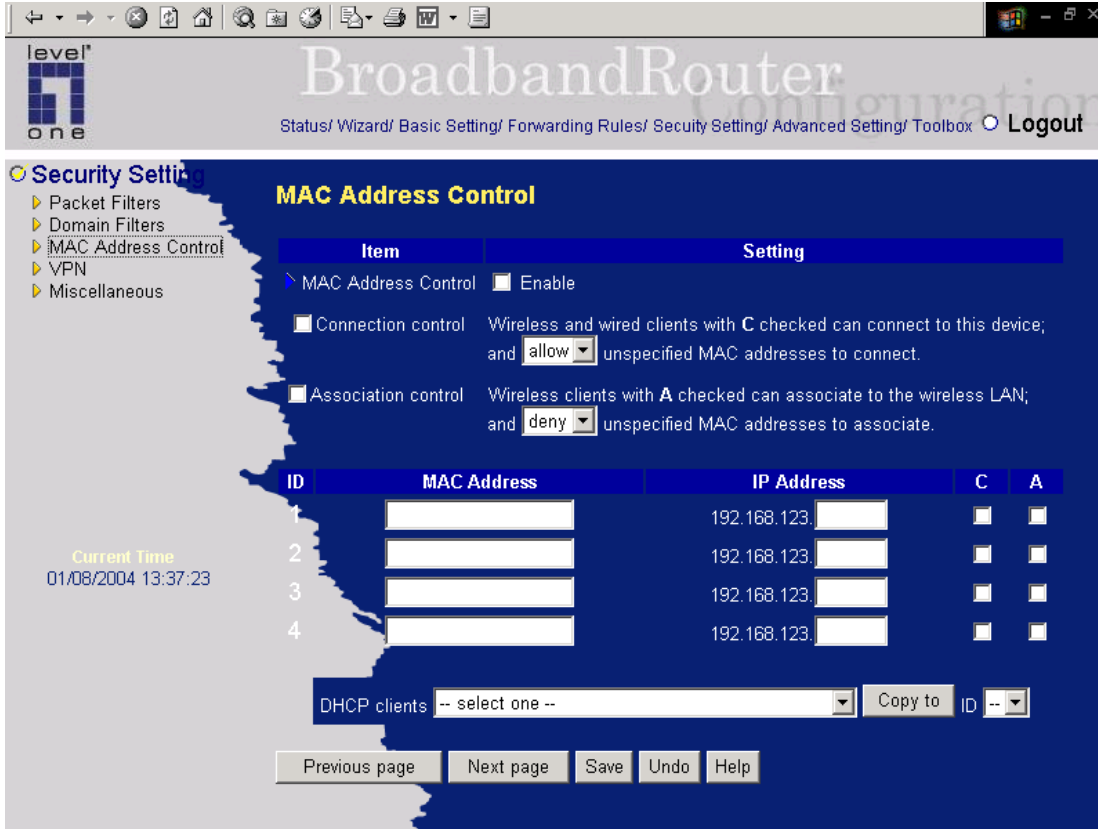
Checked to enable each rule.



In this example:

1. URL include "sex" will be blocked, and the action will be record in log-file.
2. URL include "erotica" will be blocked, but the action will be record in log-file
3. URL include "girl" will not be blocked, but the action will be record in log-file.
4. URL include "game" will be blocked, but the action will be record in log-file

4.6.4 MAC Address Control



MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

Connection control Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

Association control Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Control table

ID	MAC Address	IP Address	C	A
9	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When " Connection control " is checked, check "C" will allow the corresponding client to connect to this device.
A	When " Association control " is checked, check "A" will allow the corresponding client to associate to the wireless LAN.

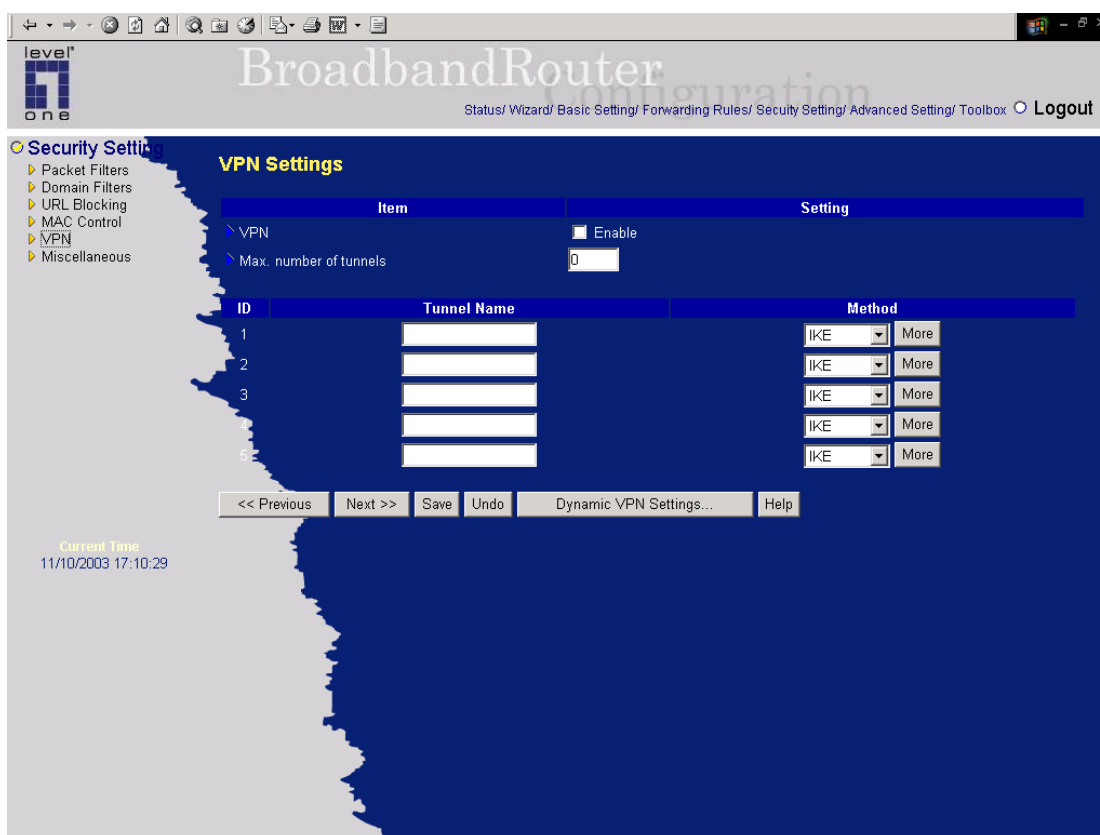
In this page, we provide the following Combobox and button to help you to input the MAC address.

DHCP clients ID

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

Previous page and Next Page To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.

4.6.5 VPN setting



VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

- **VPN enable item**

VPN protects network information from ill network inspectors. But it greatly degrades network throughput. Enable it when you really need a security tunnel. It is disabled for default.

- **Max. number of tunnels item**

Since VPN greatly degrades network throughput, the allowable maximum number of tunnels is limited. Be careful to set the value for allowing the number of tunnels can be created simultaneously. Its value ranges from 1 to 5.

- **Tunnel name**

Indicate which tunnel that is focused now.

- **Method**

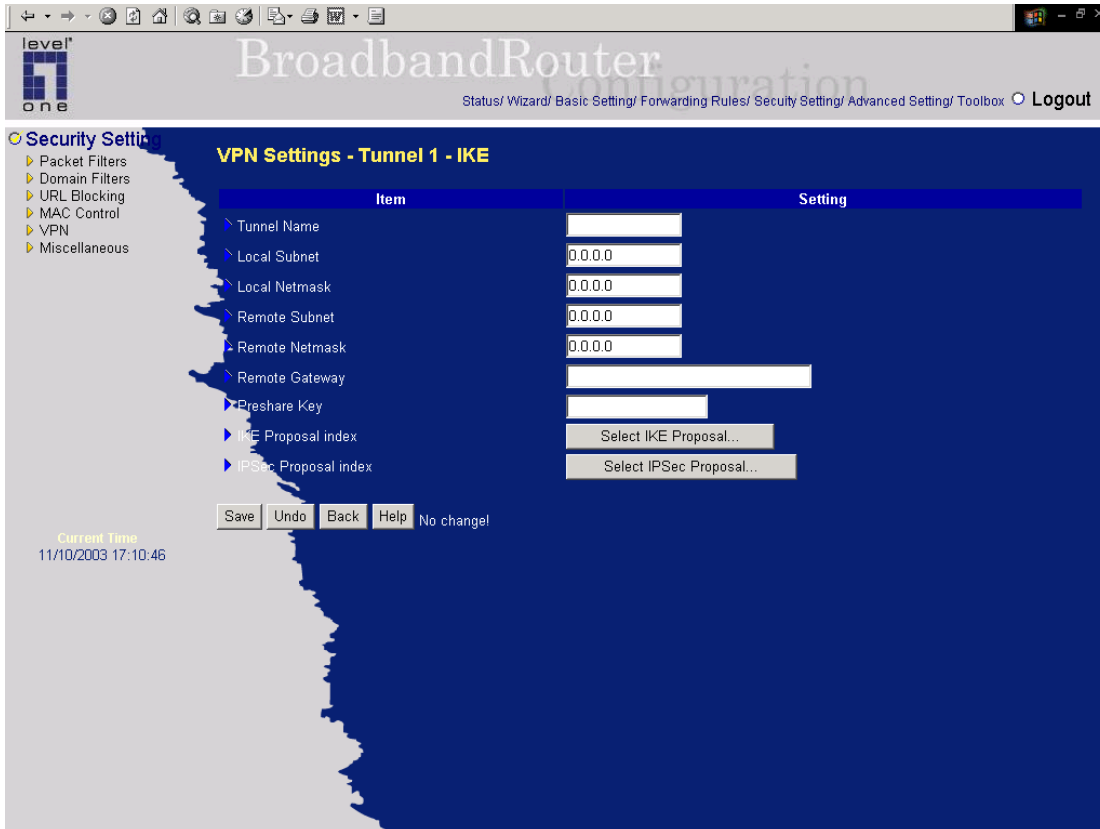
IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange.

Manual key approach indicates that two end VPN gateways setup authenticator and encryption key by system managers manually. However, IKE approach will perform automatic Internet key exchange.

System managers of both end gateways only need set the same pre-shared key.

Function of Buttons

More: To setup detailer configuration for manual key or IKE approaches by clicking the "More" button.



•VPN Settings - IKE

There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: basic setup, IKE proposal setup, and IPsec proposal setup.

Basic setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from previous page of VPN setting. IKE proposal setup includes the setting of a set of frequent-used IKE proposals and the selecting from the set of IKE proposals. Similarly, IPsec proposal setup includes the setting of a set of frequent-used IPsec proposals and the selecting from the set of IPsec proposals.

- Basic setup:

Local subnet

The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local netmask

Local netmask combined with local subnet to form a subnet domain.

Remote subnet

The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote netmask

Remote netmask combined with remote subnet to form a subnet domain of remote end.

Remote gateway

The IP address of remote VPN gateway.

Pre-shared key

The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be same for both end gateways.

Function of Buttons

Select IKE proposal: Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the dedicated tunnel. proposals for the dedicated tunnel.

Select IPSec proposal: Click the button to setup a set of frequent-used IPSec proposals and select from the set of IKE proposals for the dedicated tunnel.

The screenshot shows the configuration page for 'VPN Settings - Tunnel 1 - Set IKE Proposal'. The page has a blue header with the 'level one' logo and navigation links. A left sidebar contains a tree view for 'Security Settings'. The main content area features a table with columns for ID, Proposal Name, DH Group, Encrypt. algorithm, Auth. algorithm, Life Time, and Life Time Unit. The table contains 10 rows, each with a 'Group 1' dropdown for the DH Group and '3DES' and 'SHA1' dropdowns for the algorithms. Below the table is a 'Proposal ID' dropdown and an 'Add to Proposal index' button. At the bottom, there are 'Save', 'Undo', 'Back', and 'Help' buttons. The current time is displayed as 11/10/2003 17:12:12.

•VPN Settings - Set IKE Proposal

IKE Proposal index

A list of selected proposal indexes from the IKE proposal pool listed below. The selecting activity is performed by selecting a proposal ID and clicking "add to" button in the bottom of the page. There are only four indexes can be chosen from the proposal pool for the dedicated tunnel. Remove button beside the index list can remove selected proposal index before.

Proposal name

It indicates which IKE proposal to be focused. First char of the name with 0x00 value stands for the IKE proposal is not available.

• **DH group**

There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encryption algorithm

There are two algorithms can be selected: 3DES and DES.

Authentication algorithm

There are two algorithms can be selected: SHA1 and MD5.

Life time

The unit of life time is based on the value of Life Time Unit. If the value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds. If the value of unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways. Its value ranges from 20,480 KBs to 2,147,483,647 KBs.

Life time unit

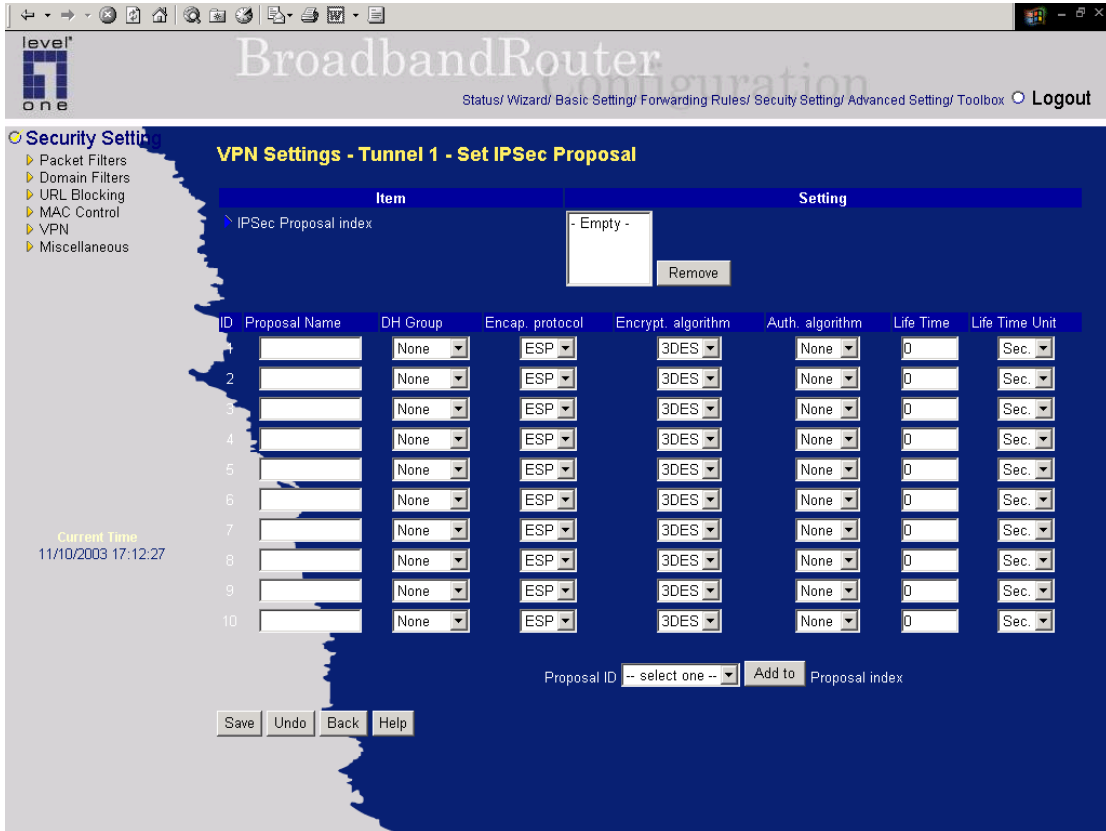
There are two units can be selected: second and KB.

Proposal ID

The identifier of IKE proposal can be chosen for adding corresponding proposal to the dedicated tunnel. There are total ten proposals can be set in the proposal pool. At most only four proposals from the pool can be applied to the dedicated tunnel as shown in the proposal index list.

Function of Buttons

Add to button: Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list. The proposals in the index list will be used in phase 1 of IKE negotiation for getting the IKSAMP SA of dedicated tunnel.



• **VPN Settings -Set IPsec Proposal**

IPsec Proposal index

A list of selected proposal indexes from the IPsec proposal pool listed below. The selecting activity is performed by selecting a proposal ID and clicking "add to" button in the bottom of the page. There are only four indexes can be chosen for the dedicated tunnel. Remove button beside the index list can remove selected proposal index before.

Proposal name

It indicates which IPsec proposal to be focused. First char of the name with 0x00 value stands for the proposal is not available.

• **DH group**

There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536). But none also can be selected here for IPsec proposal.

Encapsulation protocol

There are two protocols can be selected: ESP and AH.

Encryption algorithm

There are two algorithms can be selected: 3DES and DES. But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Authentication algorithm

There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for

IPSec proposal.

Life time

The unit of life time is based on the value of Life Time Unit. If the value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds. If the value of unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways for. Its value ranges from 20,480 KBs to 2,147,483,647 KBs.

Life time unit

There are two units can be selected: second and KB.

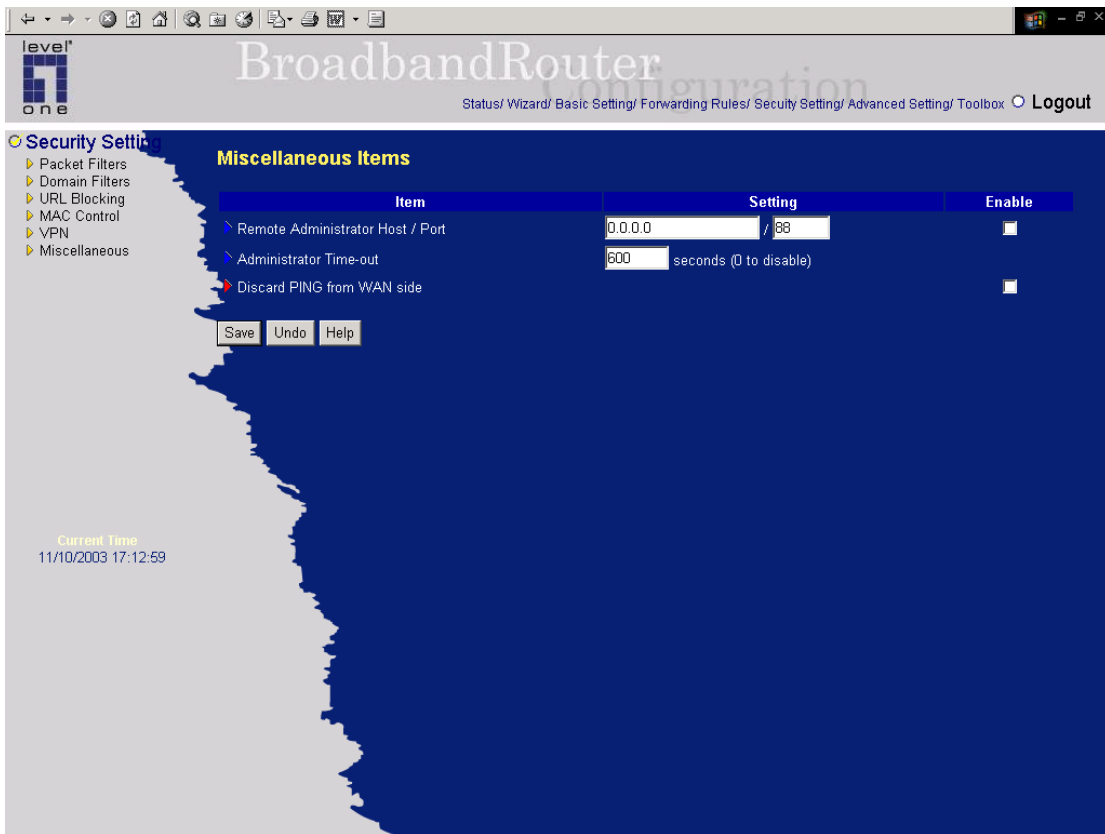
Proposal ID

The identifier of IPSec proposal can be chosen for adding the proposal to the dedicated tunnel. There are total ten proposals can be set in the proposal pool. At most only four proposals from the pool can be applied to the dedicated tunnel as shown in the proposal index list.

Function of Buttons

Add to button: Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list. The proposals in the index list will be used in phase 2 of IKE negotiation for getting the IPSec SA of dedicated tunnel.

4.6.6 Miscellaneous Items



Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

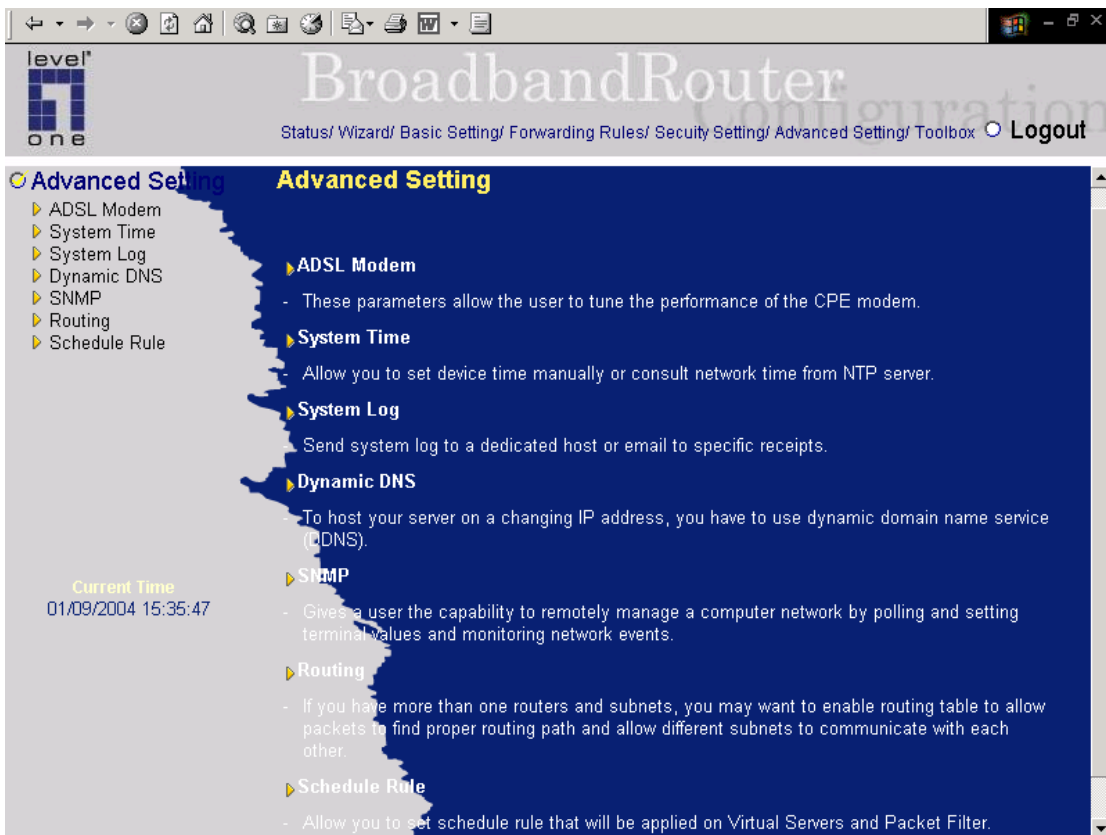
Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

4.7 Advanced Setting



The screenshot displays the configuration interface for a level one BroadbandRouter. The browser window title is "BroadbandRouter Configuration". The navigation menu includes: Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ **Advanced Setting**/ Toolbox. The "Advanced Setting" section is expanded, showing a list of sub-menus: ADSL Modem, System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule. Each sub-menu has a brief description of its function. The current time is displayed as 01/09/2004 15:35:47.

level one BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ **Advanced Setting**/ Toolbox Logout

Advanced Setting

- ▶ **ADSL Modem**
 - These parameters allow the user to tune the performance of the CPE modem.
- ▶ **System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- ▶ **System Log**
 - Send system log to a dedicated host or email to specific receipts.
- ▶ **Dynamic DNS**
 - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- ▶ **SNMP**
 - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- ▶ **Routing**
 - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- ▶ **Schedule Rule**
 - Allow you to set schedule rule that will be applied on Virtual Servers and Packet Filter.

Current Time
01/09/2004 15:35:47

4.7.1 ADSL Modem Performance Setting

The screenshot shows the configuration interface for a LevelOne BroadbandRouter. The page title is "BroadbandRouter Configuration". The navigation menu includes: Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting (selected), Toolbox, and Logout. The "Advanced Setting" menu is expanded, showing options for ADSL Modem, System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule. The "ADSL Modem Performance Setting" page contains a table with the following items and settings:

Item	Setting
Tx Gain Offset	0.0 dB
Target Noise Margin Offset	0.0 dB
Max Bits per Tone	14 bits/tonne
Rx Gain Offset	0.0 dB
Tx Output Power Offset	0.0 dBm
Rx Output Power Offset	0.0 dBm

Buttons: Save, Undo, Help, Reset to default

Current Time: 01/09/2004 15:36:13

Warning: The integrated ADSL modem might not work well if these parameters were set improperly. DO NOT try to adjust these parameters under normal usage. If any problem has happened after you changed the settings, just reset it to default values to recover the physical characteristics.

Tx Gain Offset

This parameter allows the user to add an offset on the Tx gain of the CPE Modem. The offset range is limited between -10 dB and +3 dB with a granularity of 0.5 dB. The default value is set to 0 dB, no offset.

Target Noise Margin Offset

This parameter allows the user to add an offset on the Target Noise Margin of the CPE Modem. The offset is directly added to the calculated Target Noise margin. It should be ranged between -3dB and +3dB, with a granularity of 0.5 dB. The default value is set to 0 dB, no offset.

Max Bits per Tone

The value of this parameter will limit the number of bits loaded in each upstream tone. It should be ranged between 2 and 14 bits/tonne. The default value is set to the ADSL maximum standard: 14 bits/tonne.

Rx Gain Offset

This parameter allows the user to add an offset on the Rx gain of the CPE Modem. The offset range is limited between -10 dB and +3dB with a granularity of 0.5 dB. The default value is set to 0 dB, no

offset.

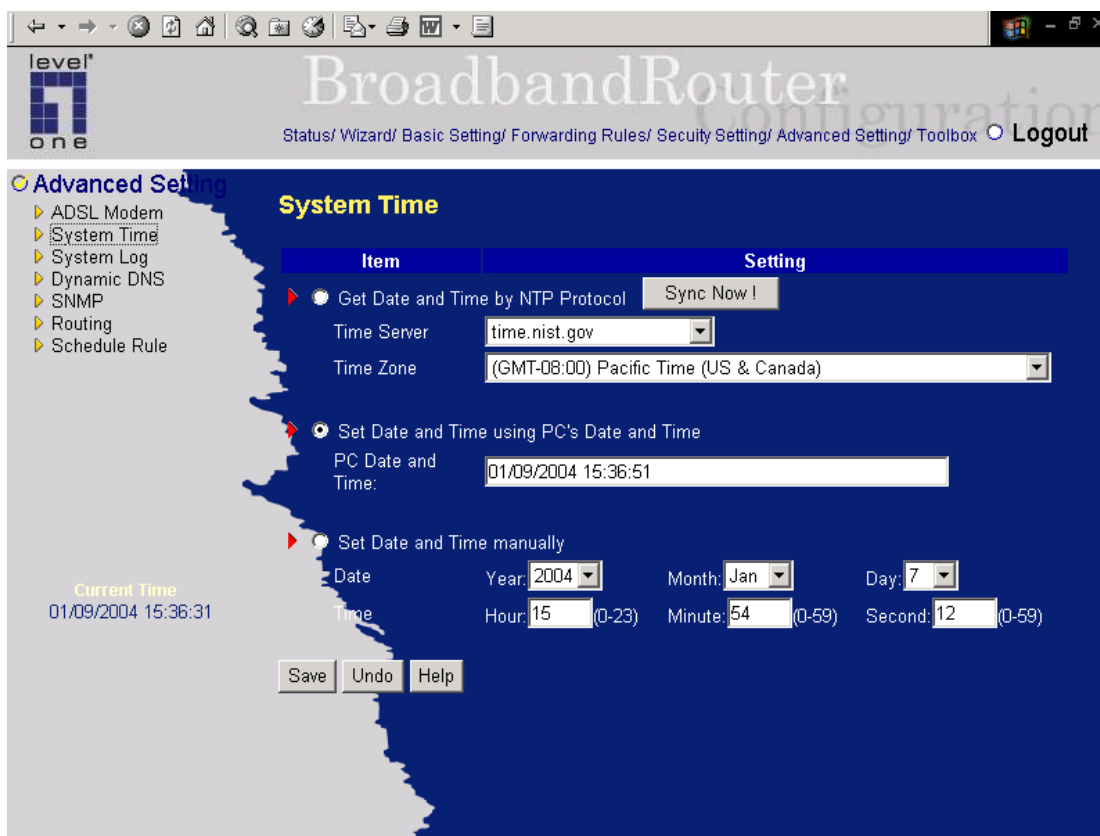
Tx Output Power Offset

This parameter allows user to reduce the Tx output power (in the upstream direction). The value should be ranged between 0 and 10 dBm.

Rx Output Power Offset

This parameter allows user to reduce the Rx output power. The value should be ranged between 0 and 10 dBm.

4.7.2 System Time



Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

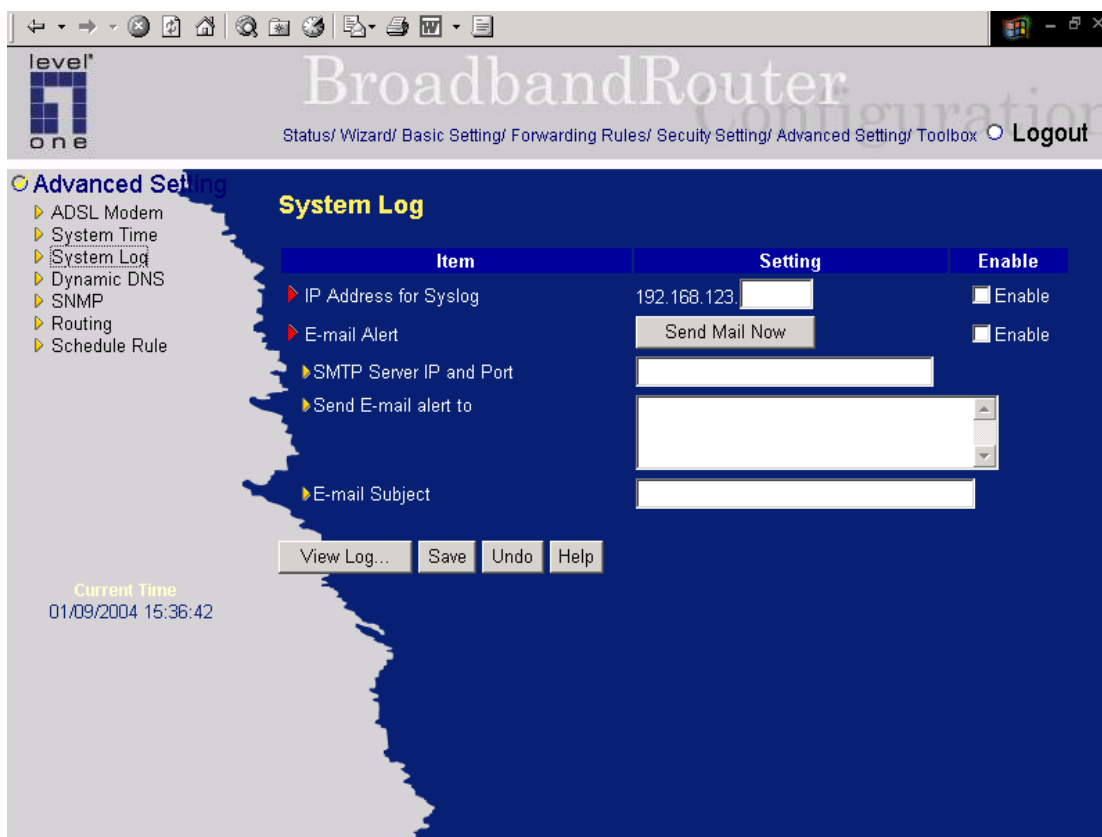
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

4.7.3 System Log



This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert(send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are contacted with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

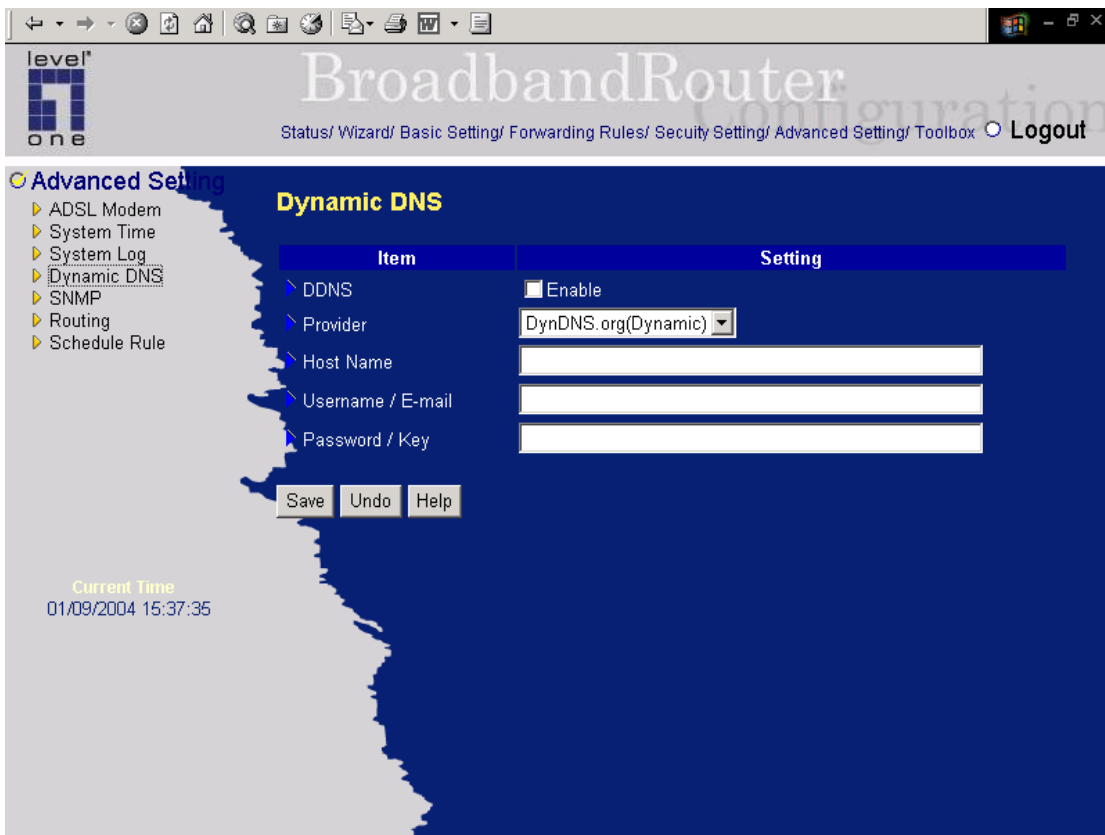
Send E-mail alert to

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert. This setting is optional.

4.7.4 Dynamic DNS



To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

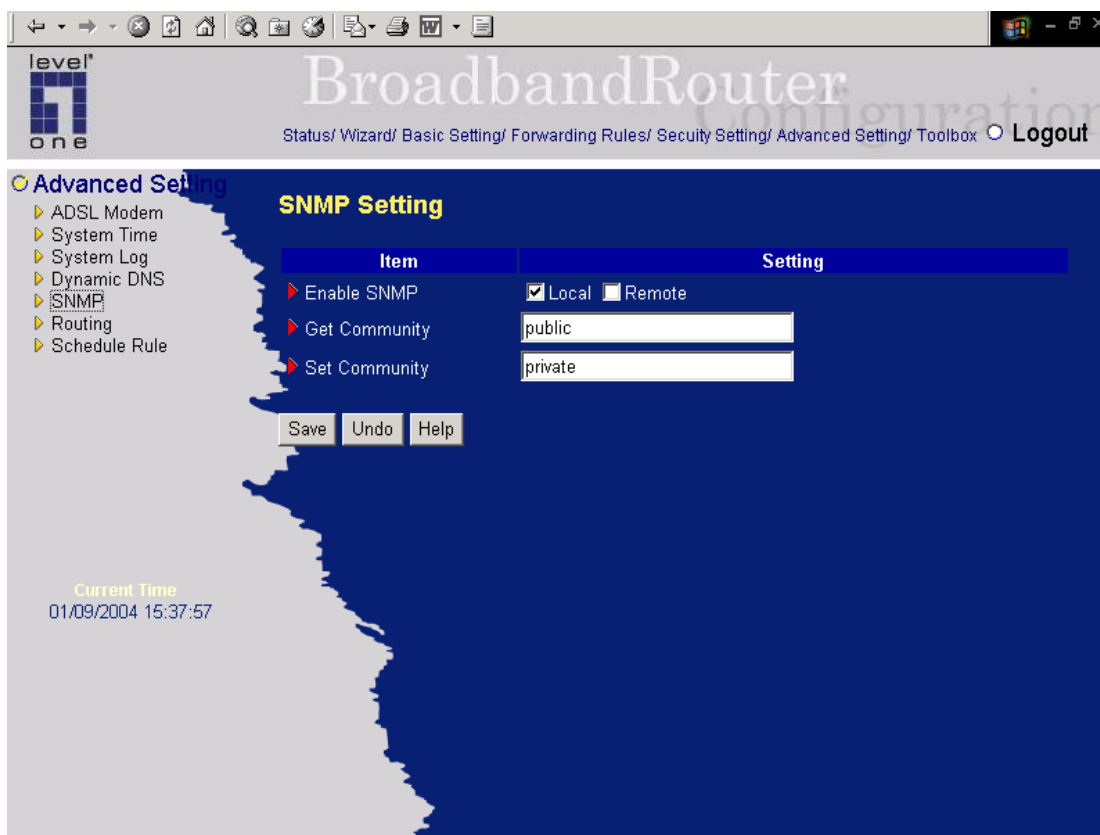
Example:



The image shows a screenshot of a 'Dynamic DNS' configuration window. The window has a dark blue background with yellow text for the title and labels. On the left side, there is a vertical list of expandable sections: 'DDNS', 'Provider', 'Host Name', 'Username / E-mail', and 'Password / Key'. Each section is preceded by a blue right-pointing arrow. To the right of these sections are the corresponding configuration fields. The 'DDNS' section is expanded and contains a checked checkbox labeled 'Enable'. The 'Provider' section contains a dropdown menu with 'DynDNS.org(Dynamic)' selected. The 'Host Name' section contains a text input field with 'user.dyndns.org'. The 'Username / E-mail' section contains a text input field with 'user'. The 'Password / Key' section contains a text input field with seven asterisks. At the bottom of the window, there are three buttons: 'Save', 'Undo', and 'Help'.

After Dynamic DNS setting is configured, click the save button.

4.7.5 SNMP Setting



In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If *Local* is checked, this device will response request from LAN. If *Remote* is checked, this device will response request from WAN.

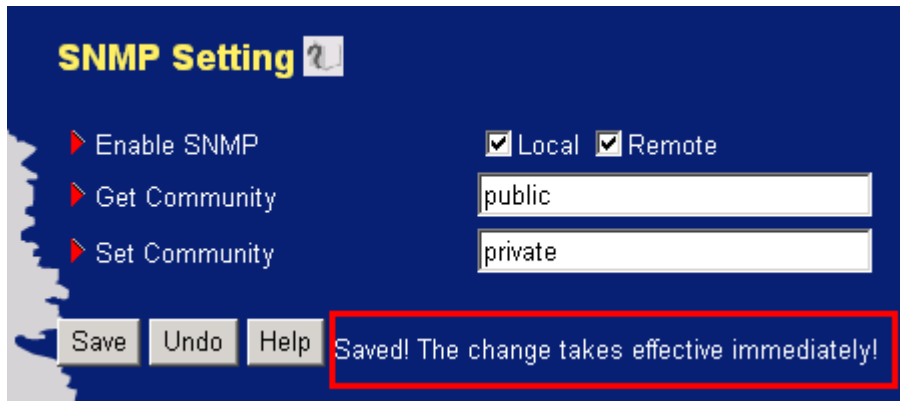
Get Community

Setting the community of GetRequest your device will response.

Set Community

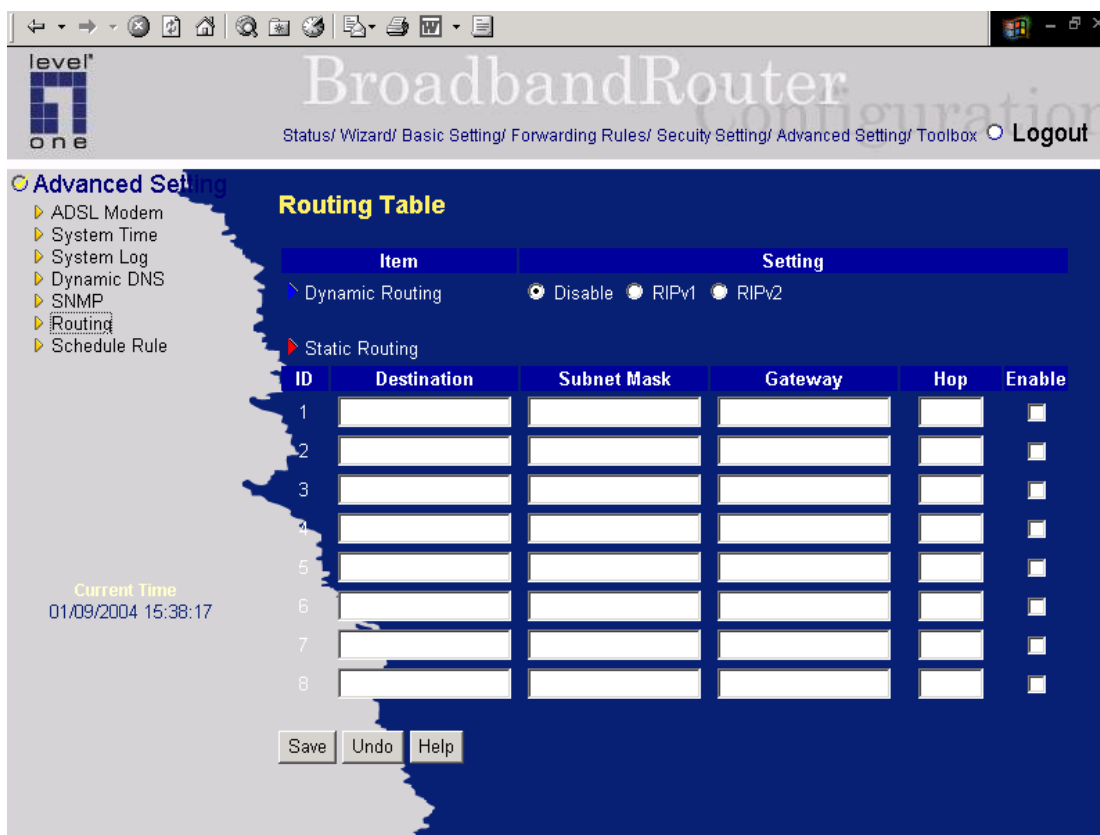
Setting the community of SetRequest your device will accept.

Example:



1. This device will response to SNMP client which's **get community** is set as “public”
2. This device will response to SNMP client which's **set community** is set as “private”
3. This device will response request from both LAN and WAN

4.7.6 Routing Table



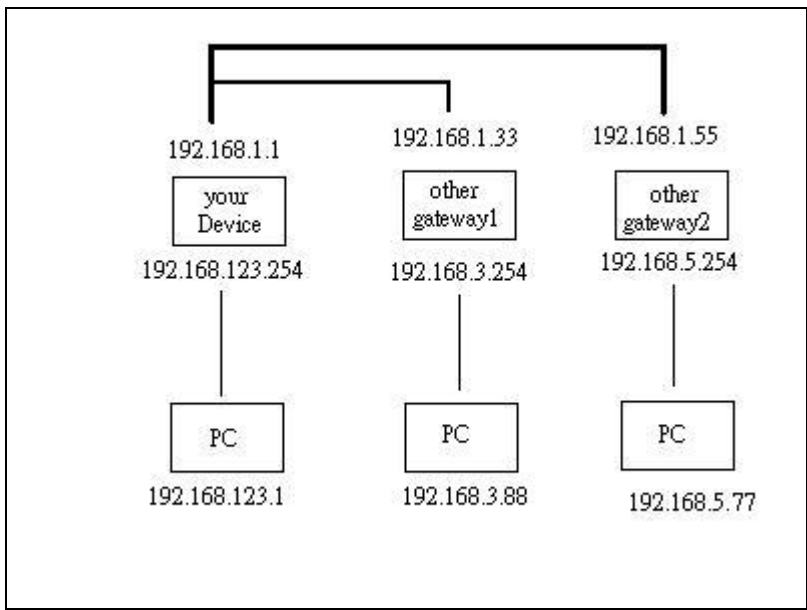
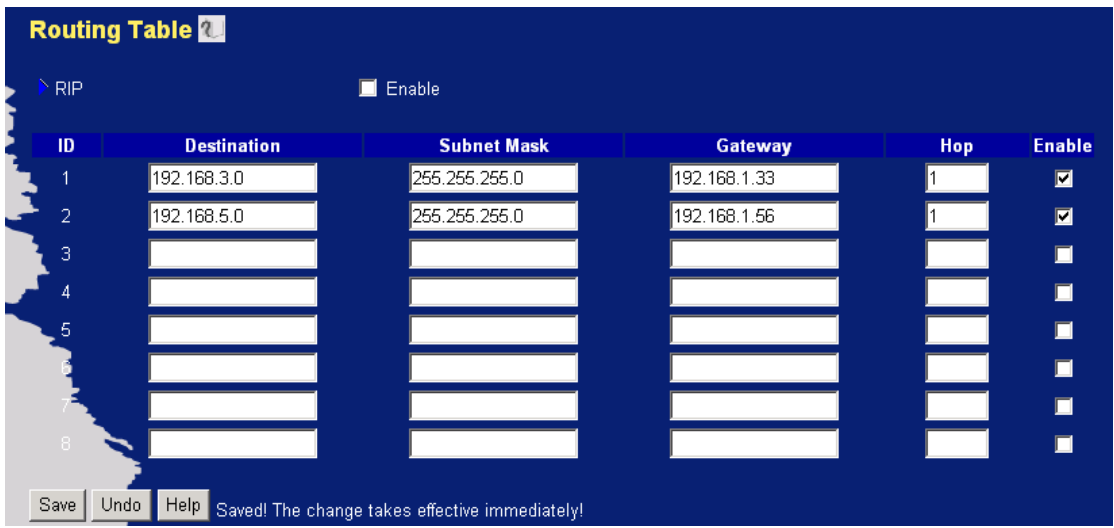
Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static and dynamic routing.

RIP Enable: Check to enable RIP function.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

Example:

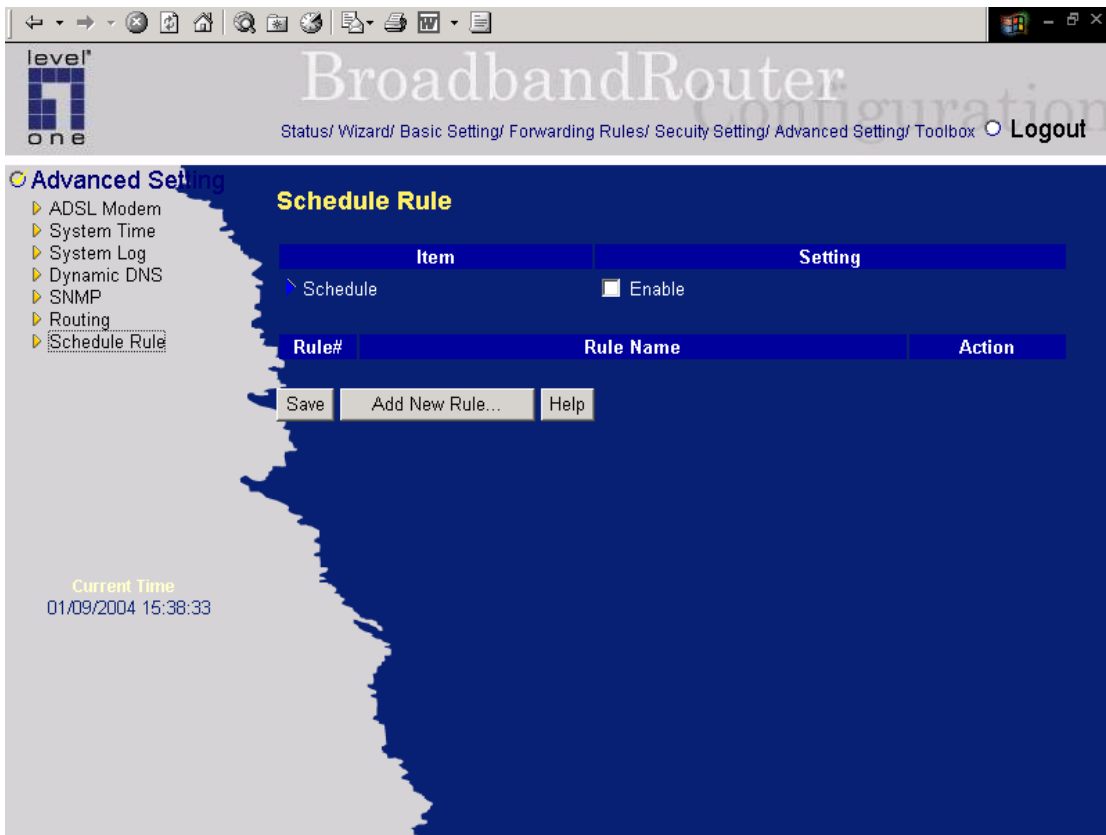


So if, for example, the host wanted to send an IP data gram to 192.168.3.88, it would use the above table to determine that it had to go via 192.168.1.33 (a gateway), And if it sends Packets to 192.168.5.77 will go via 192.168.1.55

Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

4.7.7 Schedule Rule



You can set the schedule time to decide which service at what time will be turned on or off. Select the “enable” item.

Press “Add New Rule”

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “FTP time” as everyday 14:10 to 16:20

level one
BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Advanced Setting

- ADSL Modem
- System Time
- System Log
- Dynamic DNS
- SNMP
- Routing
- Schedule Rule

Schedule Rule Setting

Name of Rule 1:

Week Day	Start Time (hh:mm)		End Time (hh:mm)	
Sunday	14	10	16	20
Monday				
Tuesday				
Wednesday				
Thursday				
Friday				
Saturday				
Every Day				

Current Time: 01/09/2004 15:39:56

Save Undo Help back

level one
BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Advanced Setting

- ADSL Modem
- System Time
- System Log
- Dynamic DNS
- SNMP
- Routing
- Schedule Rule

Schedule Rule

Schedule: Enable

Rule#	Rule Name	Action
1	FTP time	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Current Time: 01/09/2004 15:40:47

Save Add New Rule... Help

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

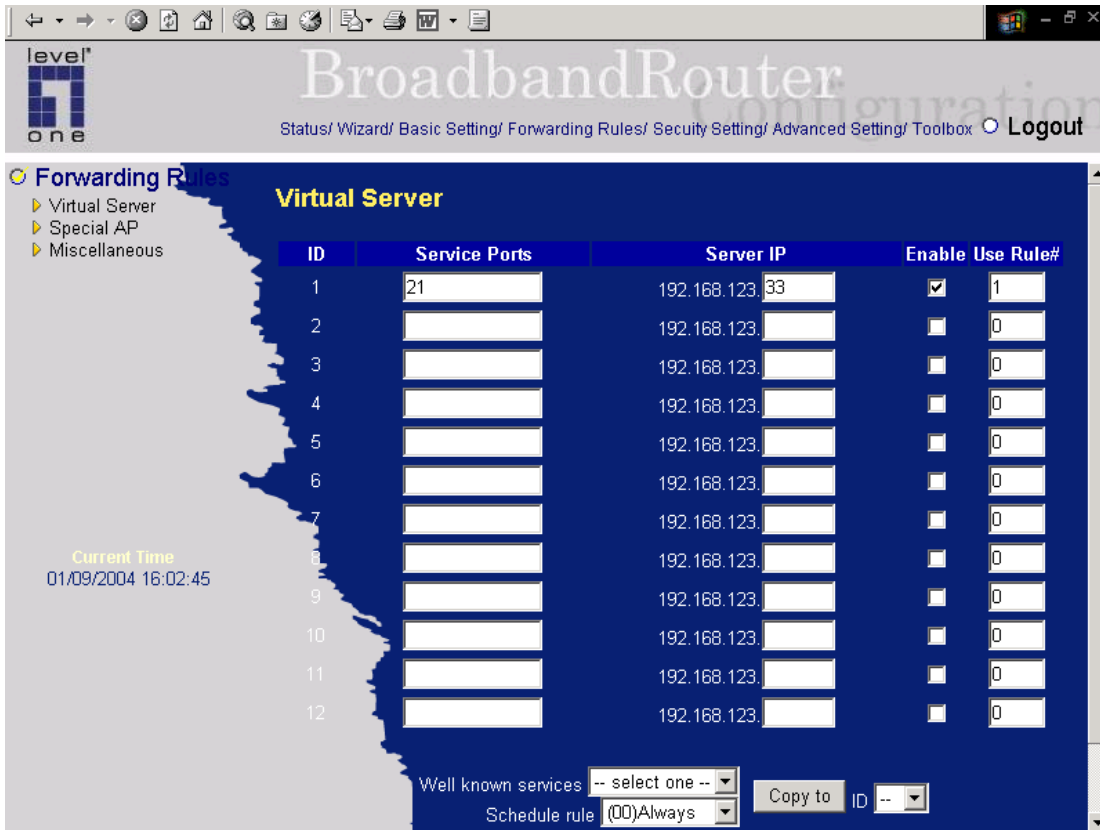
To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Example1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)



Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).

level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Settings

- Packet Filters
- Domain Filters
- MAC Address Control
- VPN
- Miscellaneous

Outbound Packet Filter

Outbound Filter Enable

Allow all to pass except those match the following rules.
 Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Use Rule#
1		21	<input checked="" type="checkbox"/>	1
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

Current Time
01/09/2004 15:31:54

Schedule rule (00)Always Copy to ID --

4.8 Toolbox

The screenshot shows a web browser window displaying the configuration interface for a level one BroadbandRouter. The browser's address bar shows the URL `http://192.168.1.1`. The page title is "BroadbandRouter Configuration". The navigation menu includes "Status", "Wizard", "Basic Setting", "Forwarding Rules", "Security Setting", "Advanced Setting", "Toolbox", and "Logout".

The "Toolbox" section is expanded, showing a list of tools:

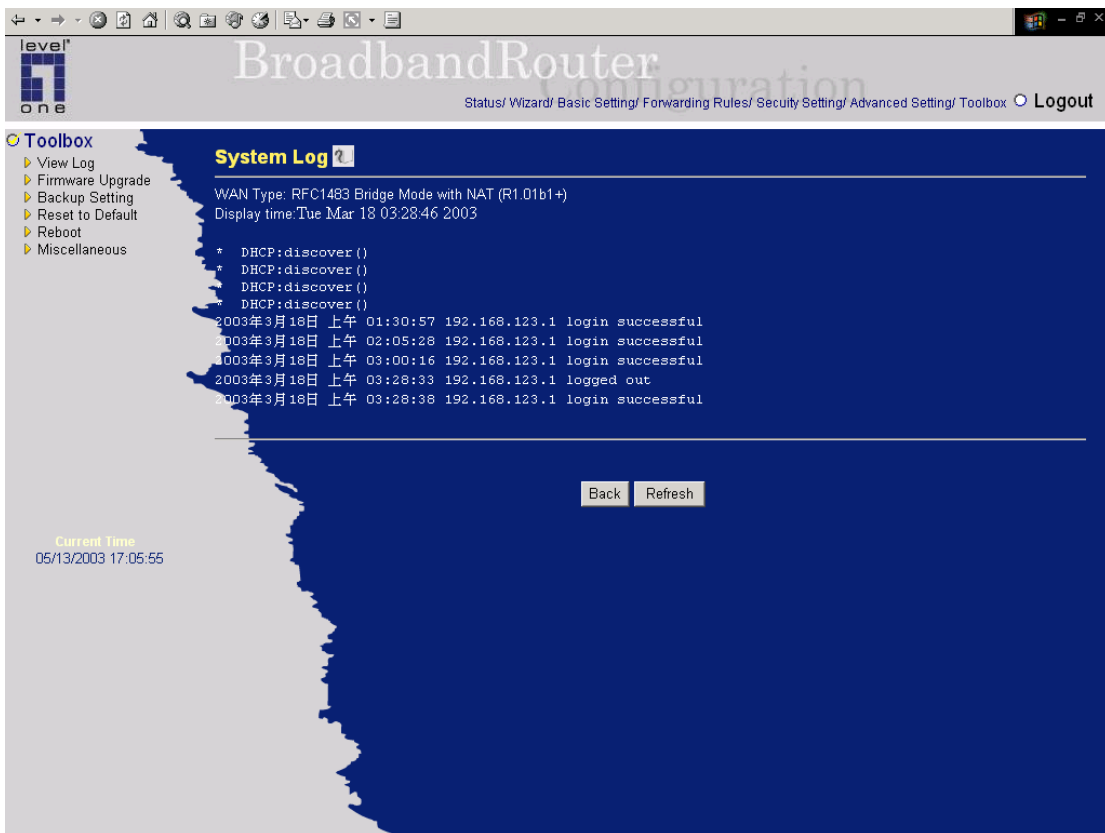
- View Log
- Firmware Upgrade
- Backup Setting
- Reset to Default
- Reboot
- Miscellaneous

The "Forwarding Rules" section is also visible, with a sub-menu for "View Log" and a list of tools:

- View Log
 - View the system logs.
- Firmware Upgrade
 - Prompt the administrator for a file and upgrade it to this device.
- Backup Setting
 - Save the settings of this device to a file.
- Reset to Default
 - Reset the settings of this device to the default values.
- Reboot
 - Reboot this device.
- Miscellaneous
 - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
 - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

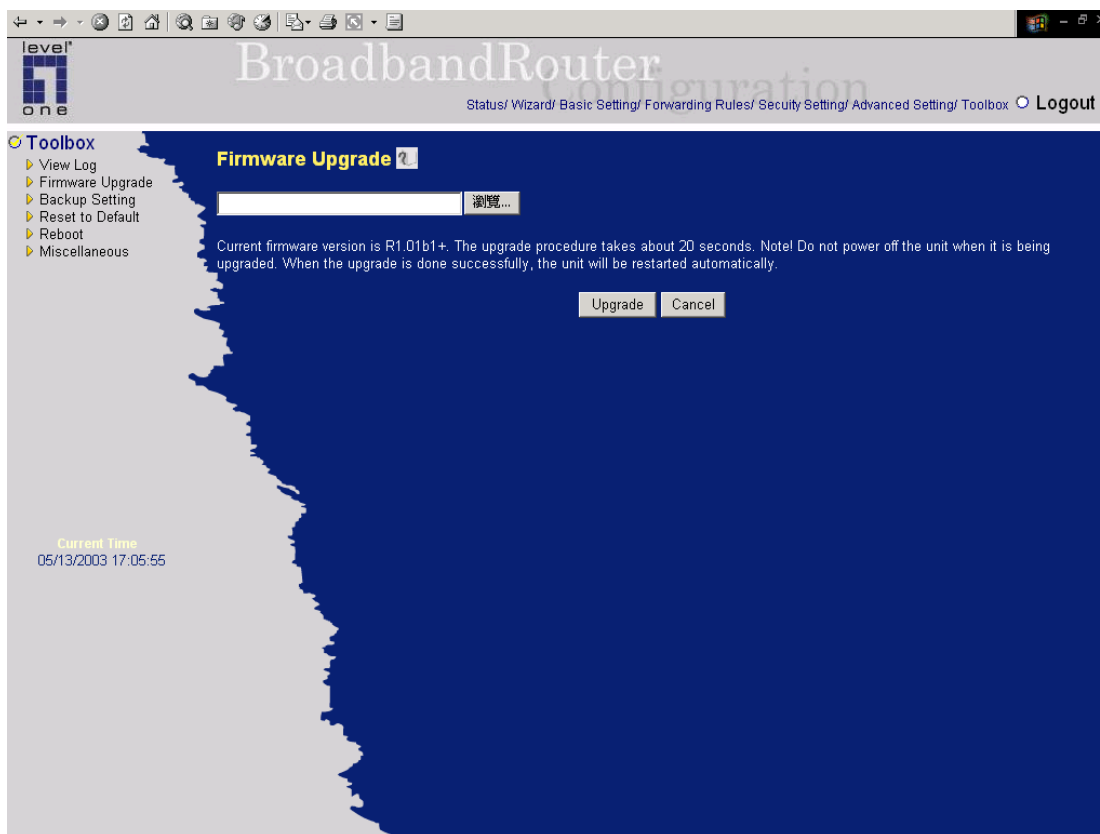
The current time is displayed as 05/13/2003 17:05:55.

4.8.1 View Log



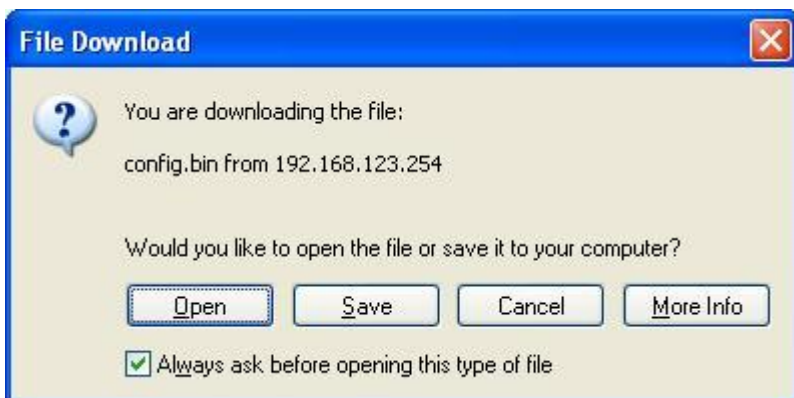
You can View system log by clicking the **View Log** button

4.8.2 Firmware Upgrade



You can upgrade firmware by clicking **Firmware Upgrade** button.

4.8.3 Backup Setting



You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

4.8.4 Reset to default



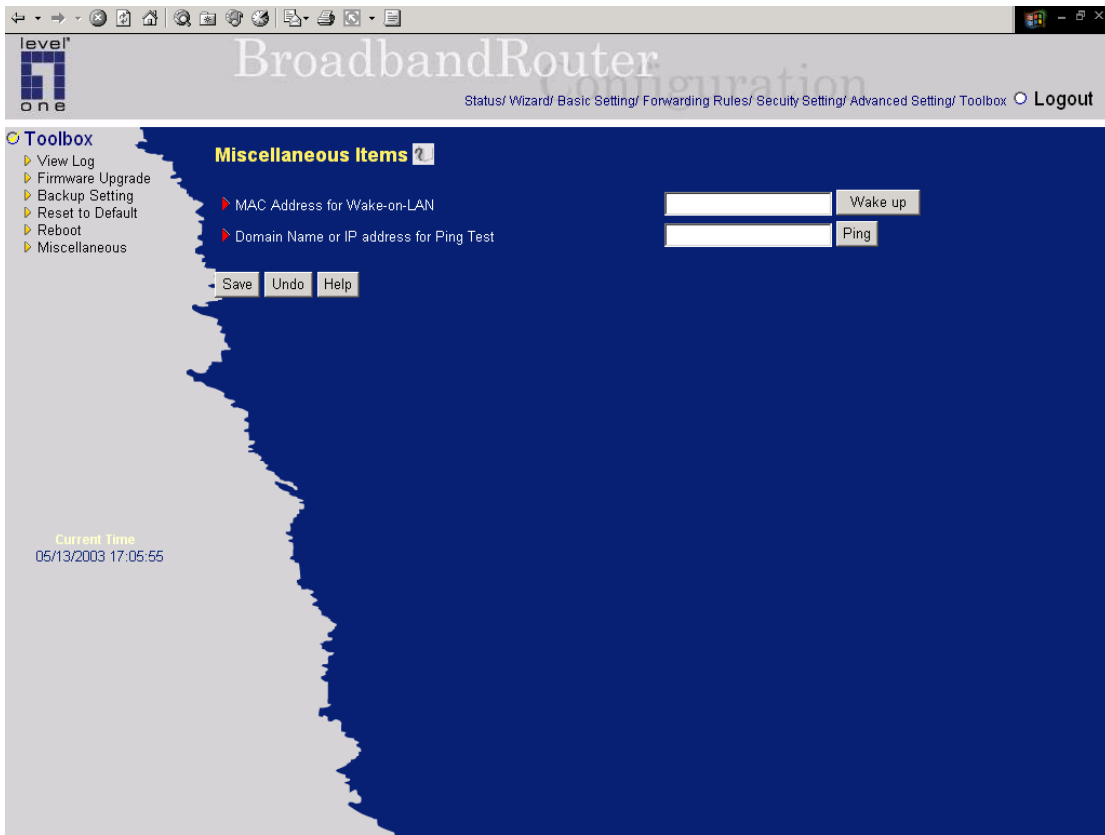
You can also reset this product to factory default by clicking the **Reset to default** button.

4.8.5 Reboot



You can also reboot this product by clicking the **Reboot** button.

4.8.6 Miscellaneous Items



MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP address for Ping Test

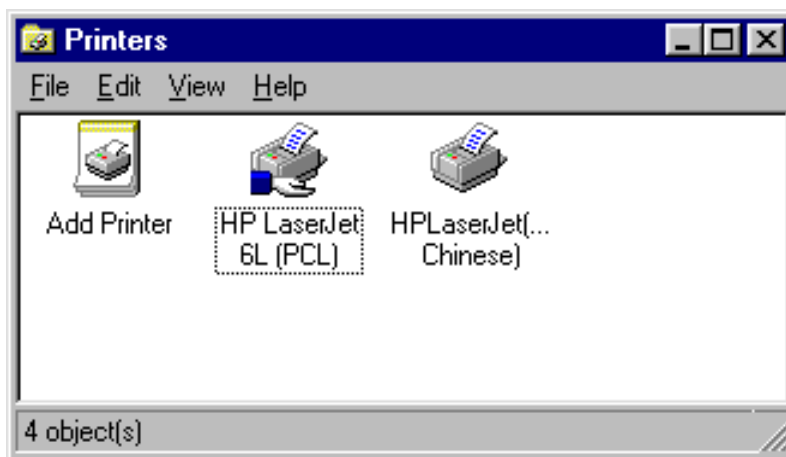
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Chapter 5 Print Server

WBR-3402 provides the function of network print server for MS Windows 95/98/NT/2000 and Unix based platforms. (If the product you purchased doesn't have printer port, please skip this chapter.)

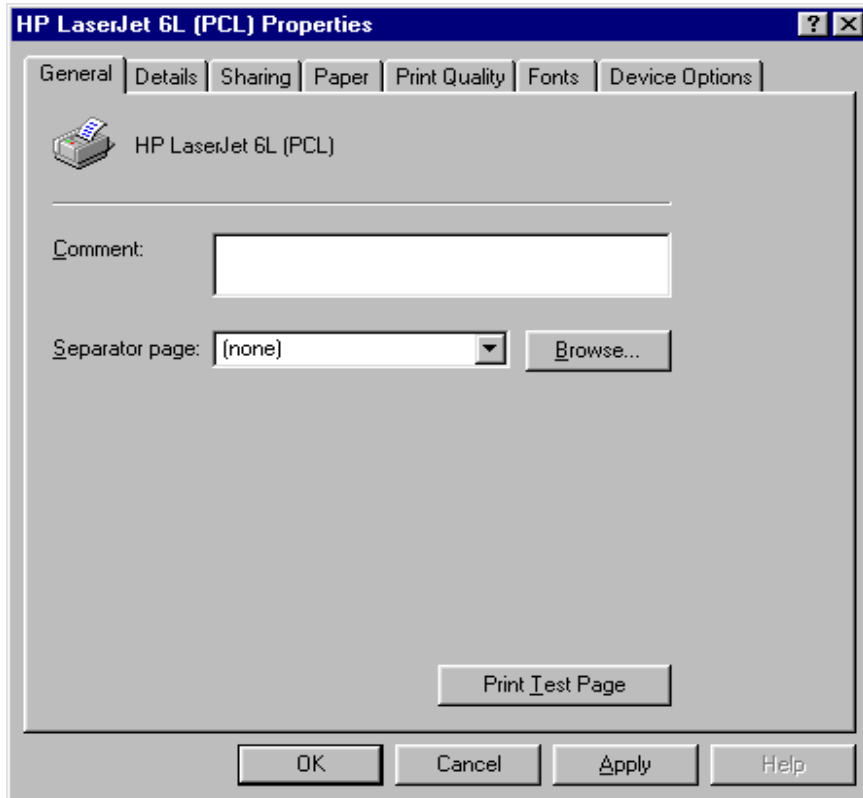
5.1 Configuring on Windows 95/98 Platforms

After you finished the software installation procedure described in Chapter 3, your computer has possessed the network printing facility provided by this product. For convenience, we call the printer connected to the printer port of this product as server printer. On a Windows 95/98 platform, open the **Printers** window in the **My Computer** menu:

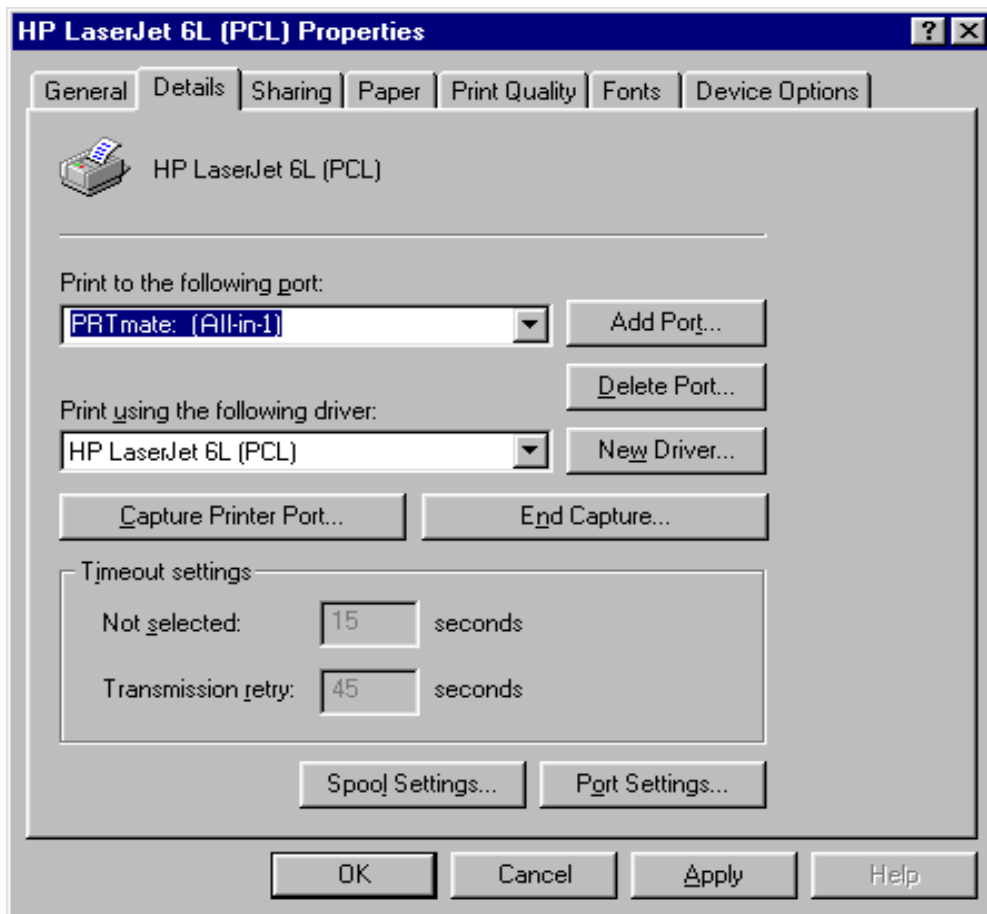


Now, you can configure the print server of this product:

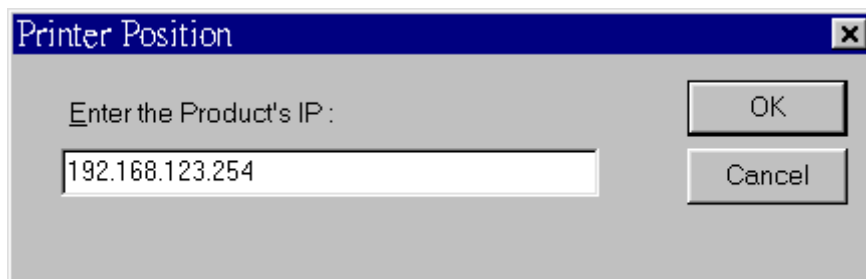
1. Find out the corresponding icon of your server printer, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the **Properties** item:



2. Click the **Details** item:



3. Choose the "PRTmate: (All-in-1)" from the list attached at the **Print To** item. Be sure that the **Printer Driver** item is configured to the correct driver of your server printer.
4. Click on the button of **Port Settings**:

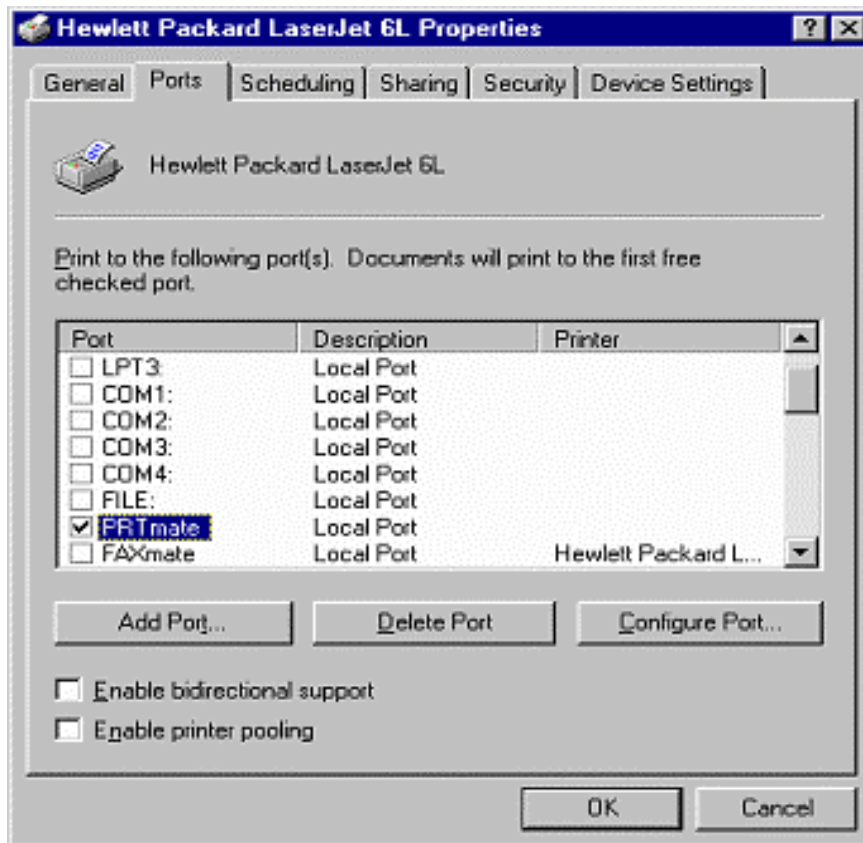


Type in the IP address of this product and then click the **OK** button.

8. Make sure that all settings mentioned above are correct and then click the **OK** button.

5.2 Configuring on Windows NT Platforms

The configuration procedure for a Windows NT platform is similar to that of Windows 95/98 except the screen of printer **Properties**:



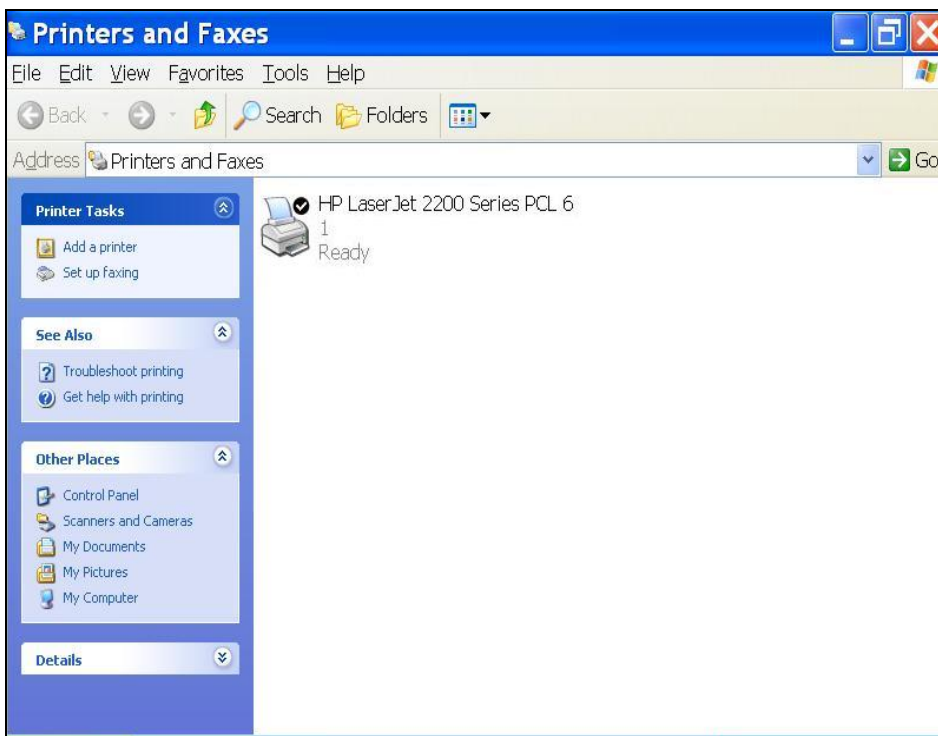
Compared to the procedure in last section, the selection of **Details** is equivalent to the selection of **Ports**, and **Port Settings** is equivalent to **Configure Port**.

5.3 Configuring on Windows 2000 and XP Platforms

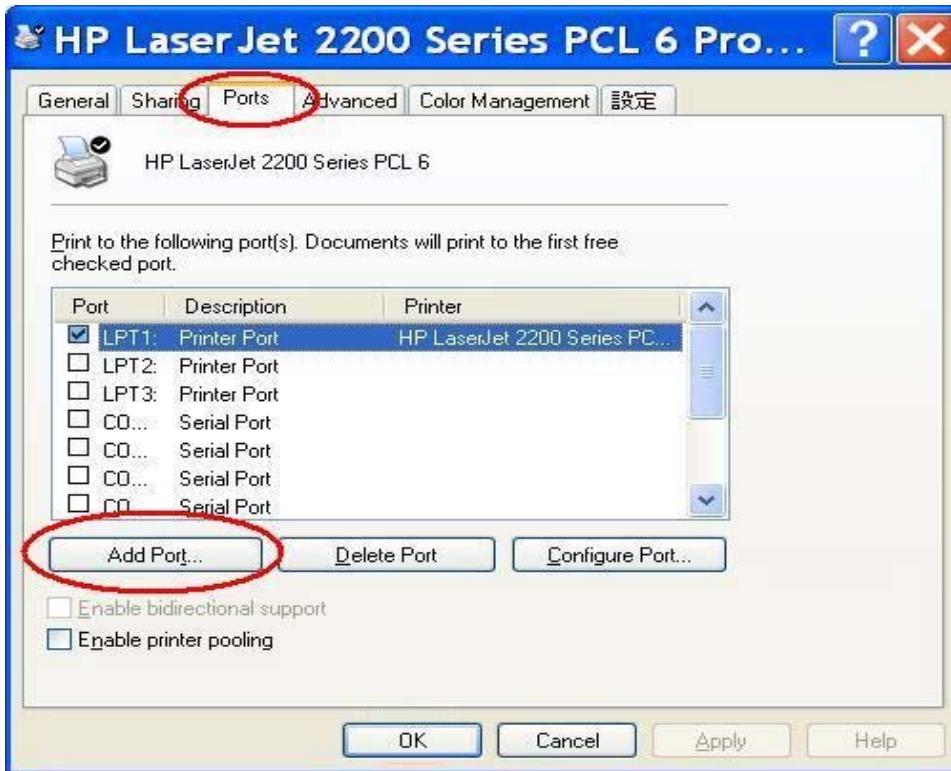
Windows 2000 and XP have built-in LPR client, users could utilize this feature to Print.

You have to install your Printer Driver on LPT1 or other ports before you proceed the following sequence.

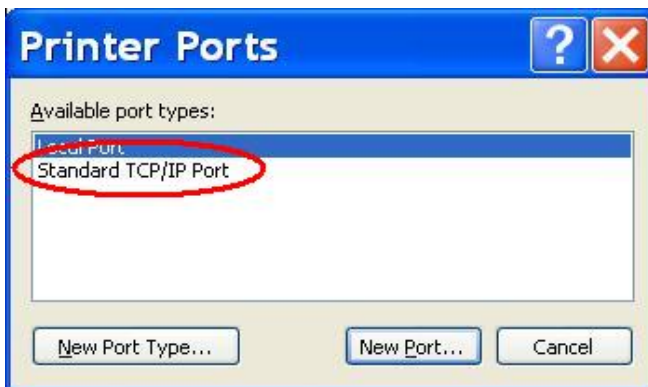
1. Open Printers and Faxes.



2. Select "Ports" page, Click "Add Port..."



3. Select "Standard TCP/IP Port", and then click "New Port..."



4. Click Next and then provide the following information:

Type address of server providing LPD that is our NAT device: 192.168.123.254

Add Standard TCP/IP Printer Port Wizard

Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.123.254

Port Name: IP_192.168.123.254

< Back Next > Cancel

4. Select Custom, then click “Settings...”

Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required
The device could not be identified.

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

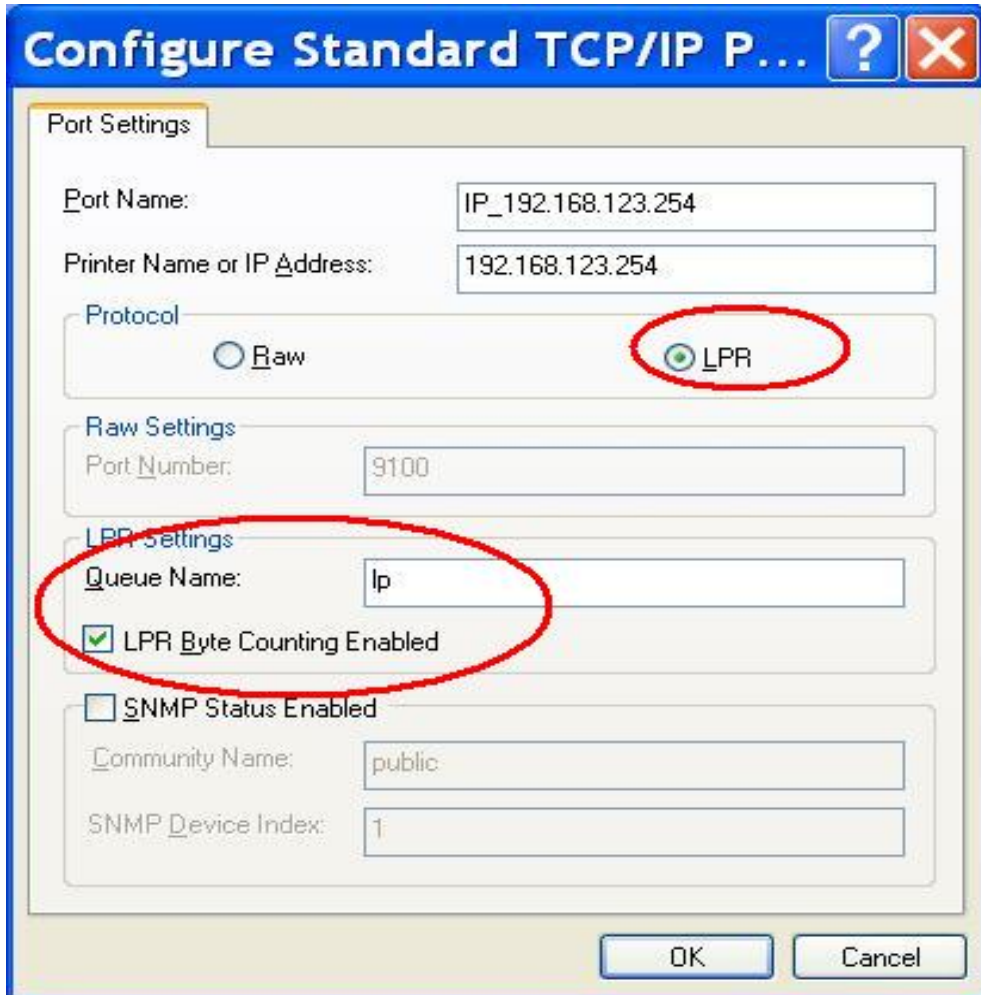
Standard Generic Network Card

Custom Settings...

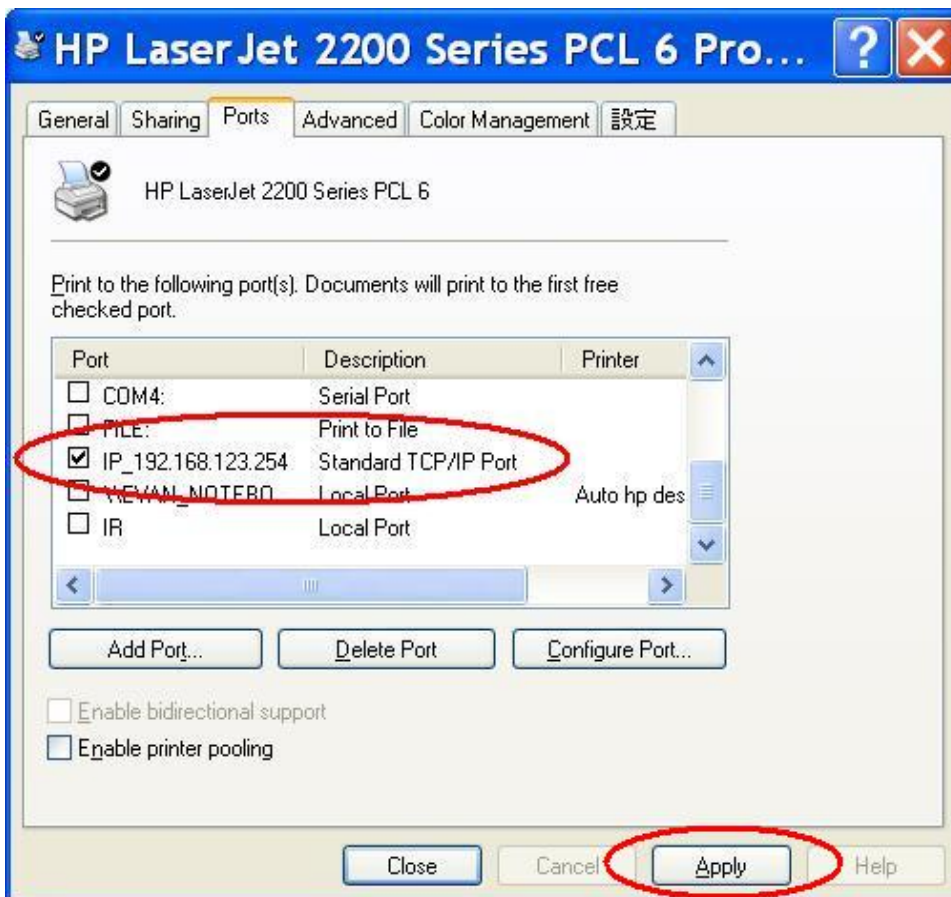
< Back Next > Cancel

6. Select "LPR", type "lp" lowercase letter in "Queue Name:"

And enable "LPR Byte Counting Enabled".



7. Apply your settings



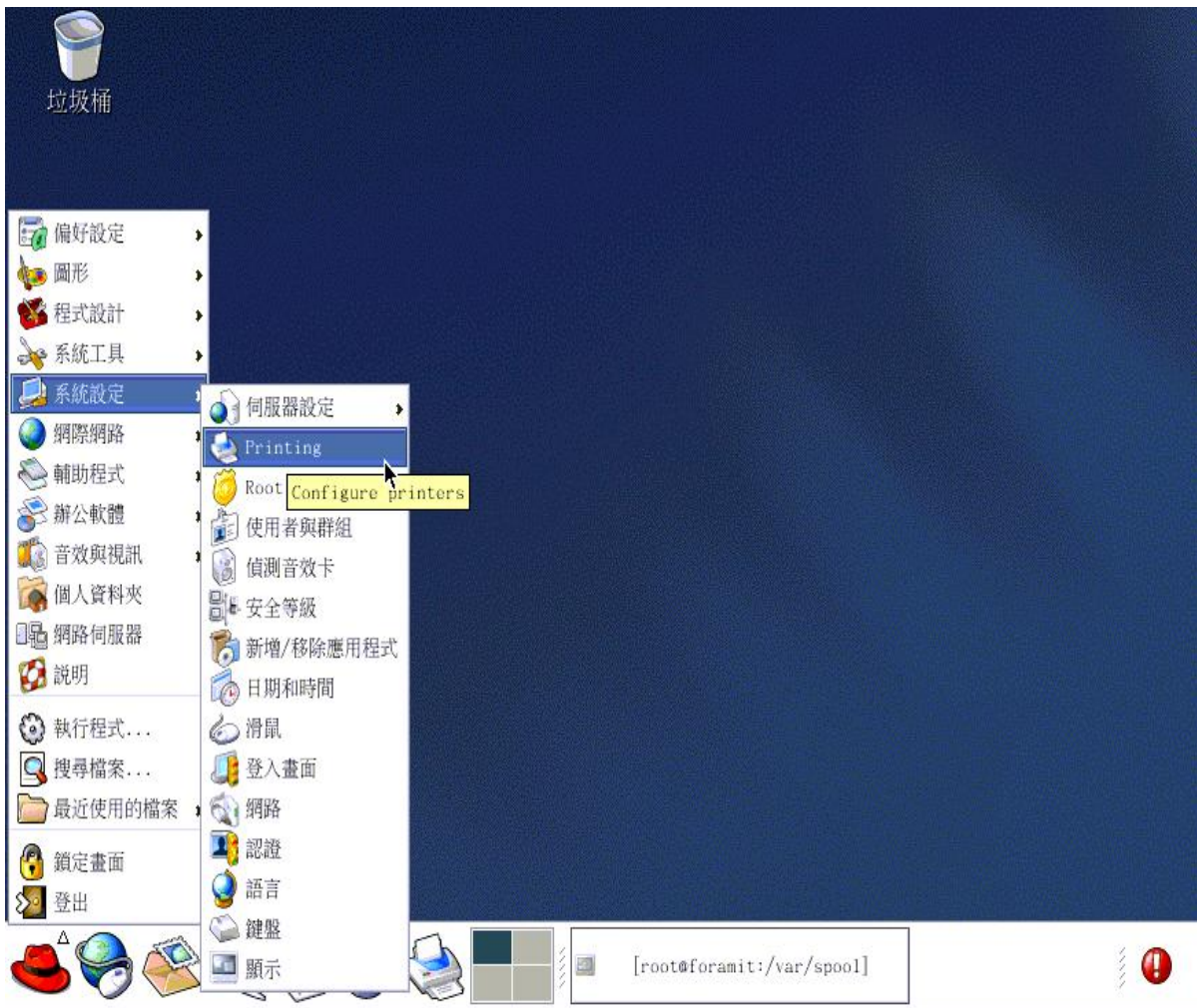
5.4 Configuring on Unix-like based Platforms

Please follow the traditional configuration procedure on Unix platforms to setup the print server of this product. The printer name is “lp.”

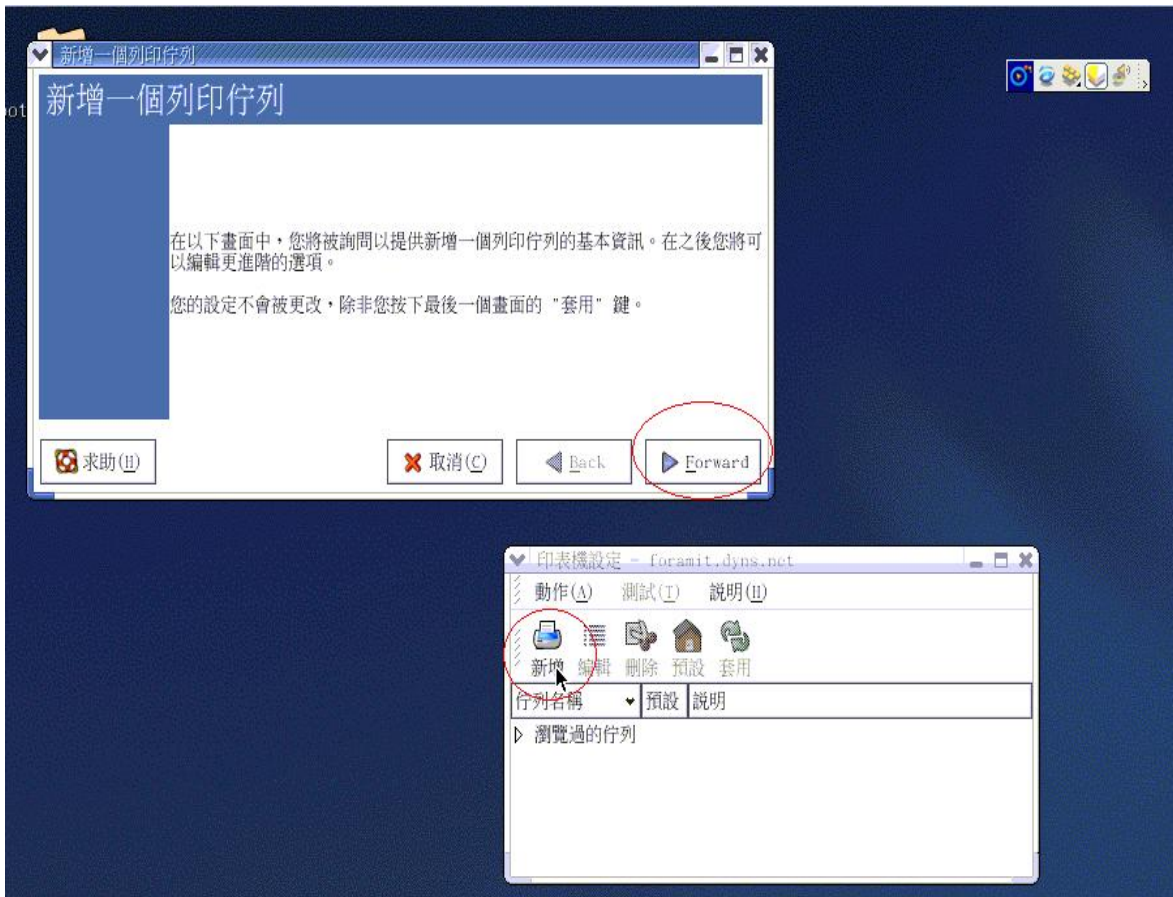
In X-Windows, for example, In Redhat Platforms,

Please follow the below steps to configure your printer on Red Hat 9.0.

1. Start from the Red Hat---> System Setting---> Printing.



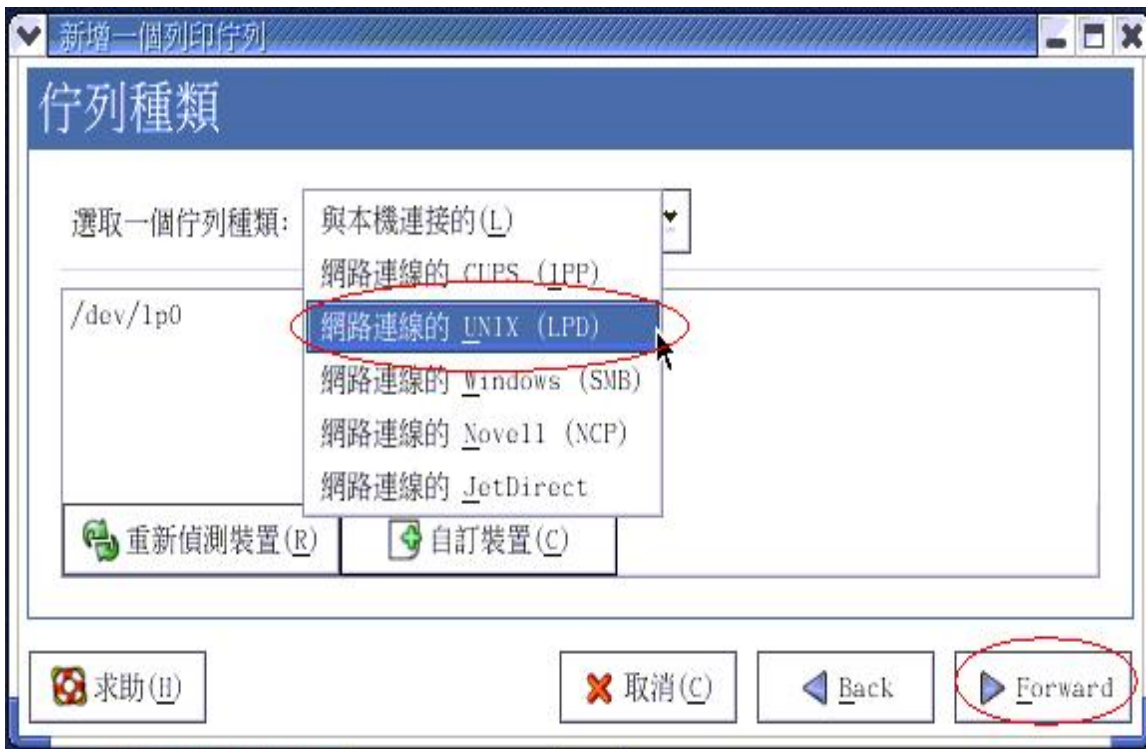
2. Click Add--> Forward.



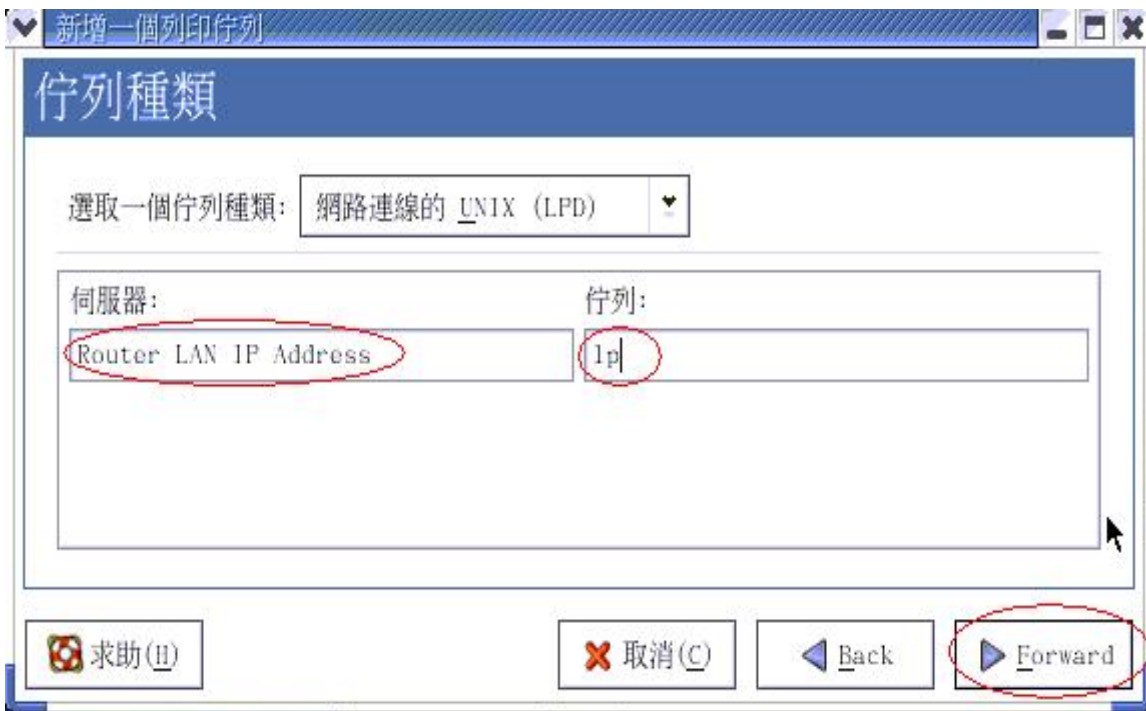
3. Enter the Printer Name, Comments then forward.



4. Select LPD protocol and then forward.



5. Enter the router LAN IP Address and the queue name "lp". Then forward.



6. Select the Printer Brand and Model Name. Then Forward.



7. Click Apply to finish setup.



8. At last you must click Apply on the toolbox to make the change take effective.



In Command Mode:

Linux has built-in LPR client ,You can utilize it for printing.

You can manual set it or via the tool "printtool" in X-windows.

PS: The spool name is "lp"-----all lowercase letter.

Below is my setting.

/etc/printcap

```
-----  
lp:\  
:sd=/var/spool/lpd/lp:\  
:mx#0:\  
:sh:\  
:rm=192.168.123.254:\  
:rp=lp:\ ----->key point  
:if=/var/spool/lpd/lp/filter:  
-----
```

Then add the corresponding directory

```
#mkdir /var/spool/lpd/lp
```

Too see the detail ,please refer to the online manual in linux.

```
#man printcap
```

5.5 Configuring on Apple PC

1.First, go to Printer center (Printer list) and add printer



2.Choose **IP print** and setup **printer ip address** (router Lan ip address).

3.Disable “**Default Queue of Server.**” And fill in ‘**lp**’ in Queue name item.

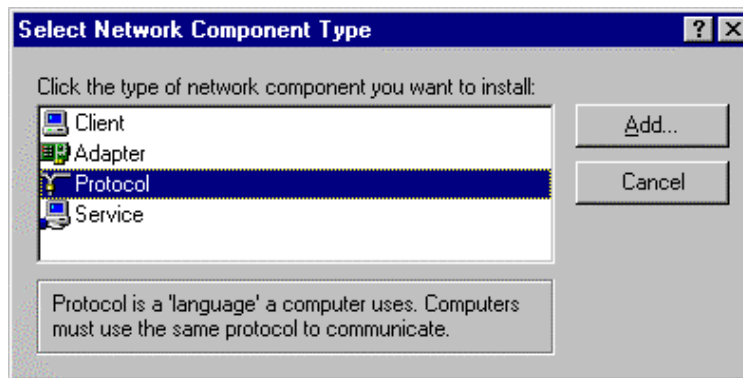
4.Printer type: Choose “**General**”.

Appendix A TCP/IP Configuration for Windows 95/98

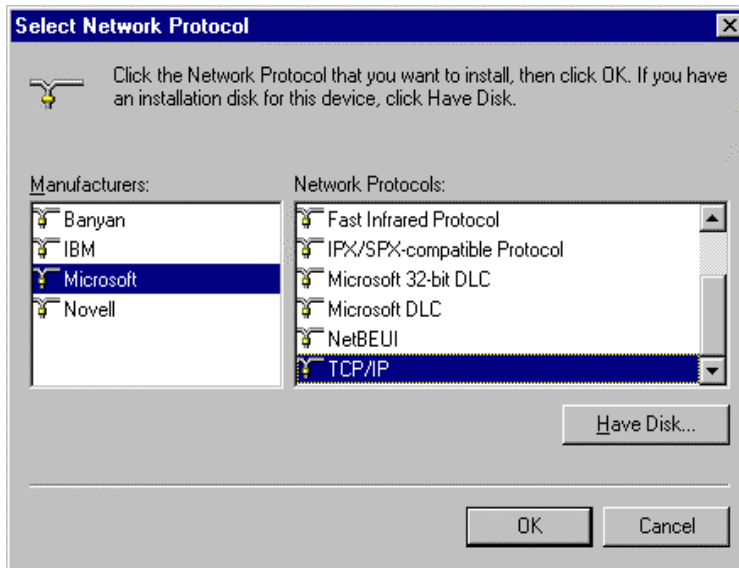
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



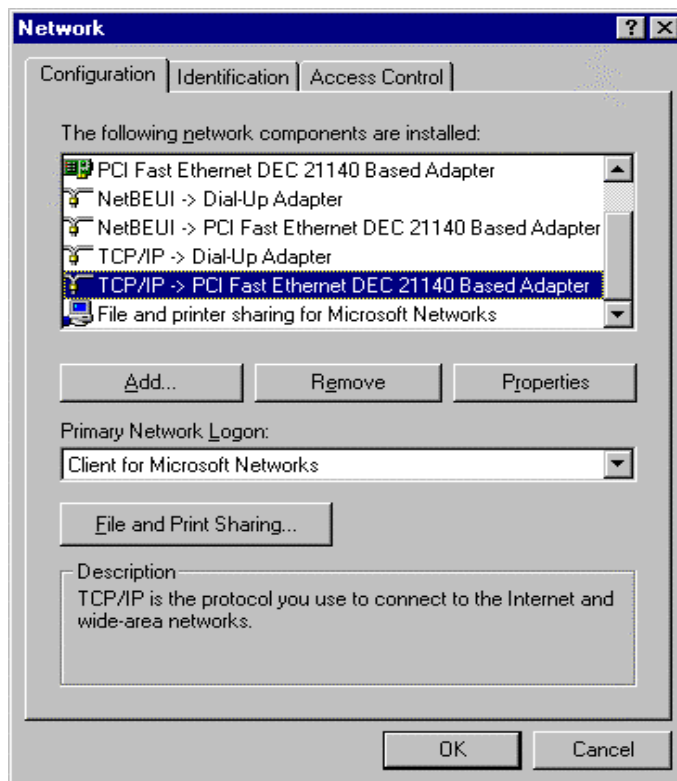
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

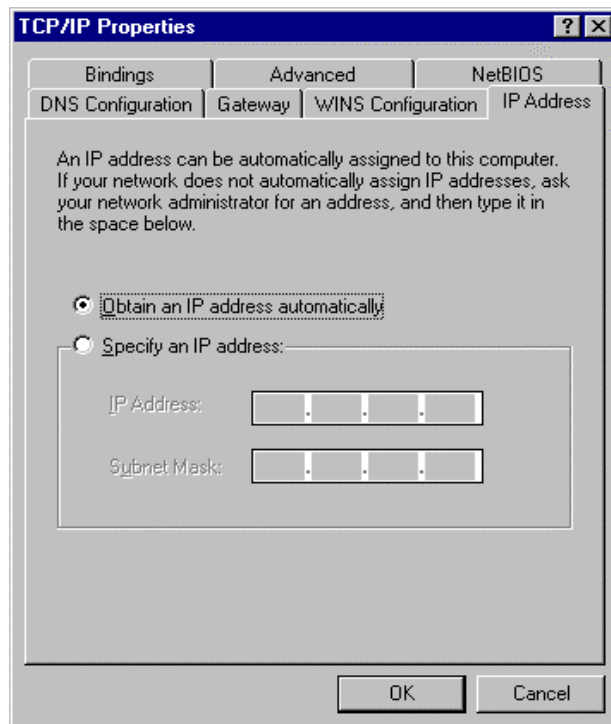
A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.

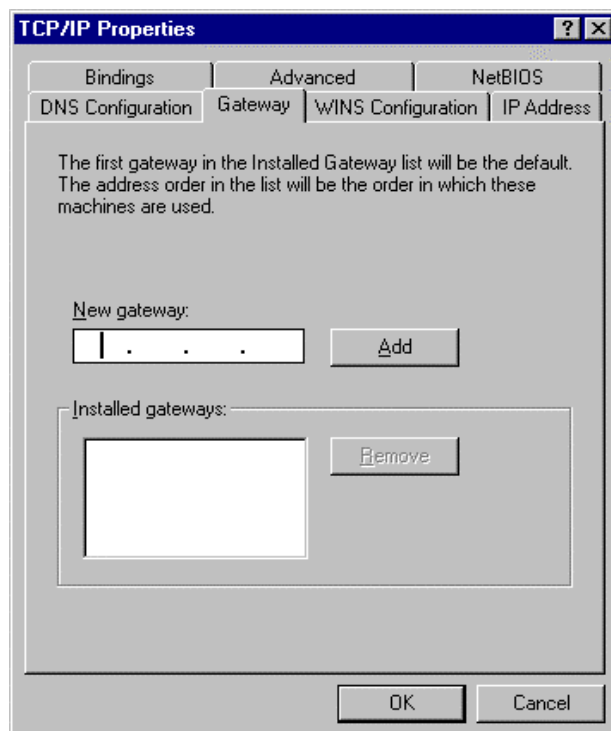


3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:

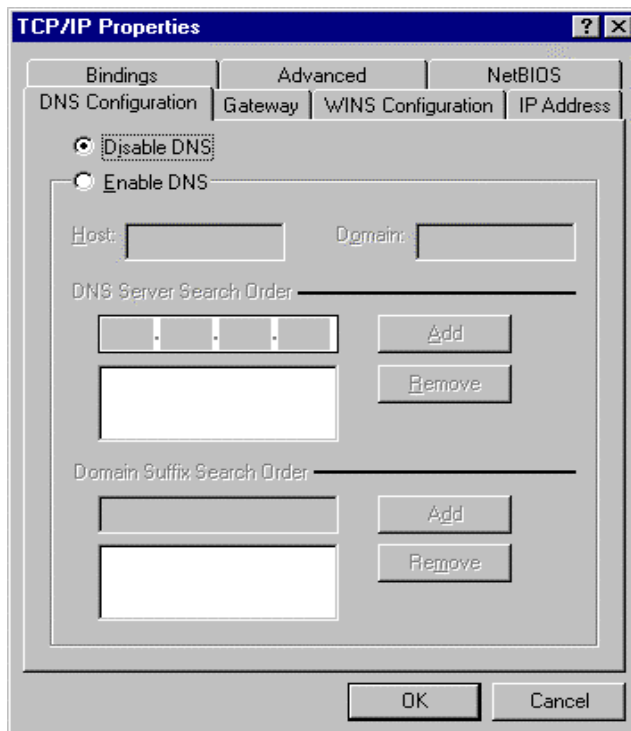
- a. Select **Obtain an IP address automatically** in the IP Address tab.



- b. Don't input any value in the Gateway tab.

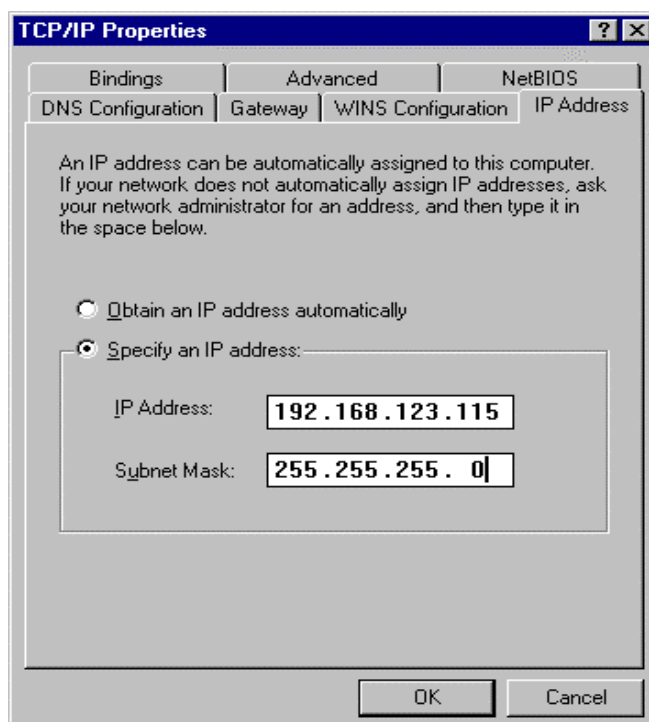


- c. Choose **Disable DNS** in the DNS Configuration tab.

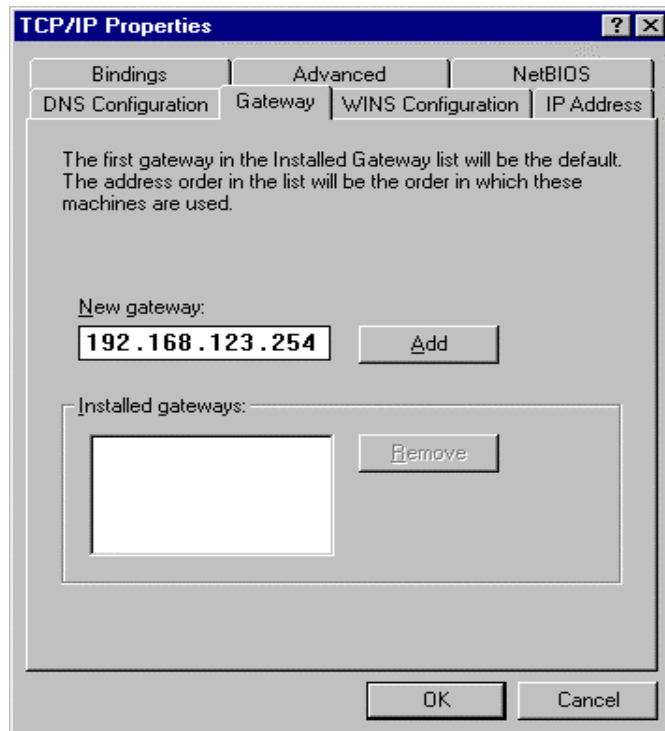


B. Configure IP manually

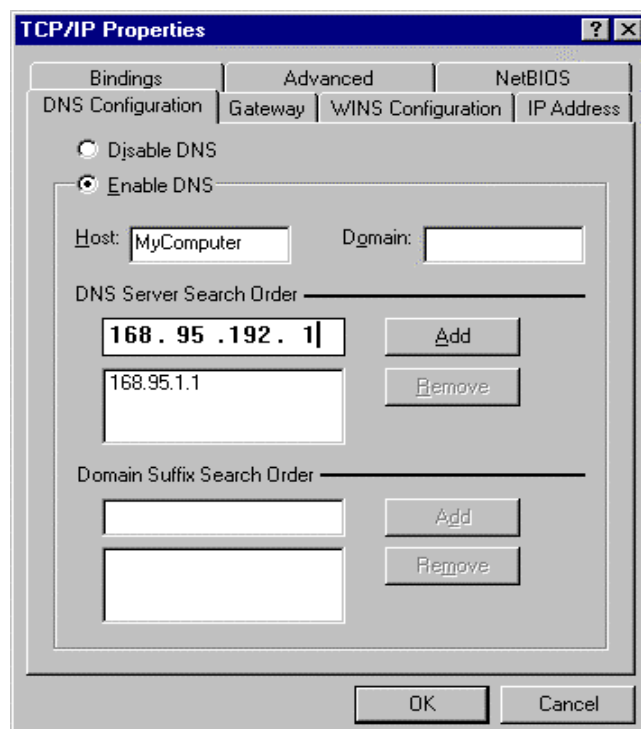
- a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



- b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.



- c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.



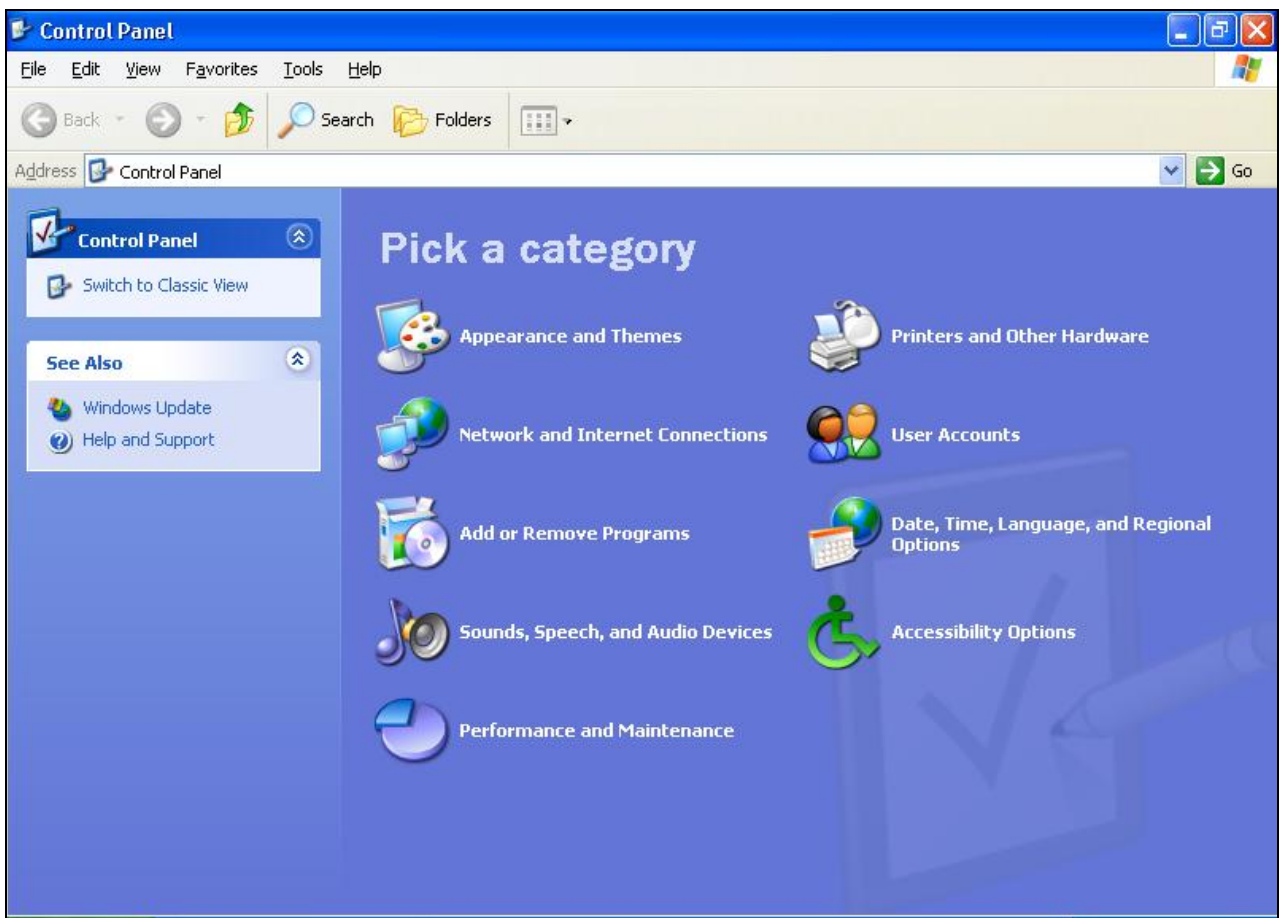
Appendix B Win 2000/XP IPSEC Setting guide

Example: Win XP/2000 →VPN Router

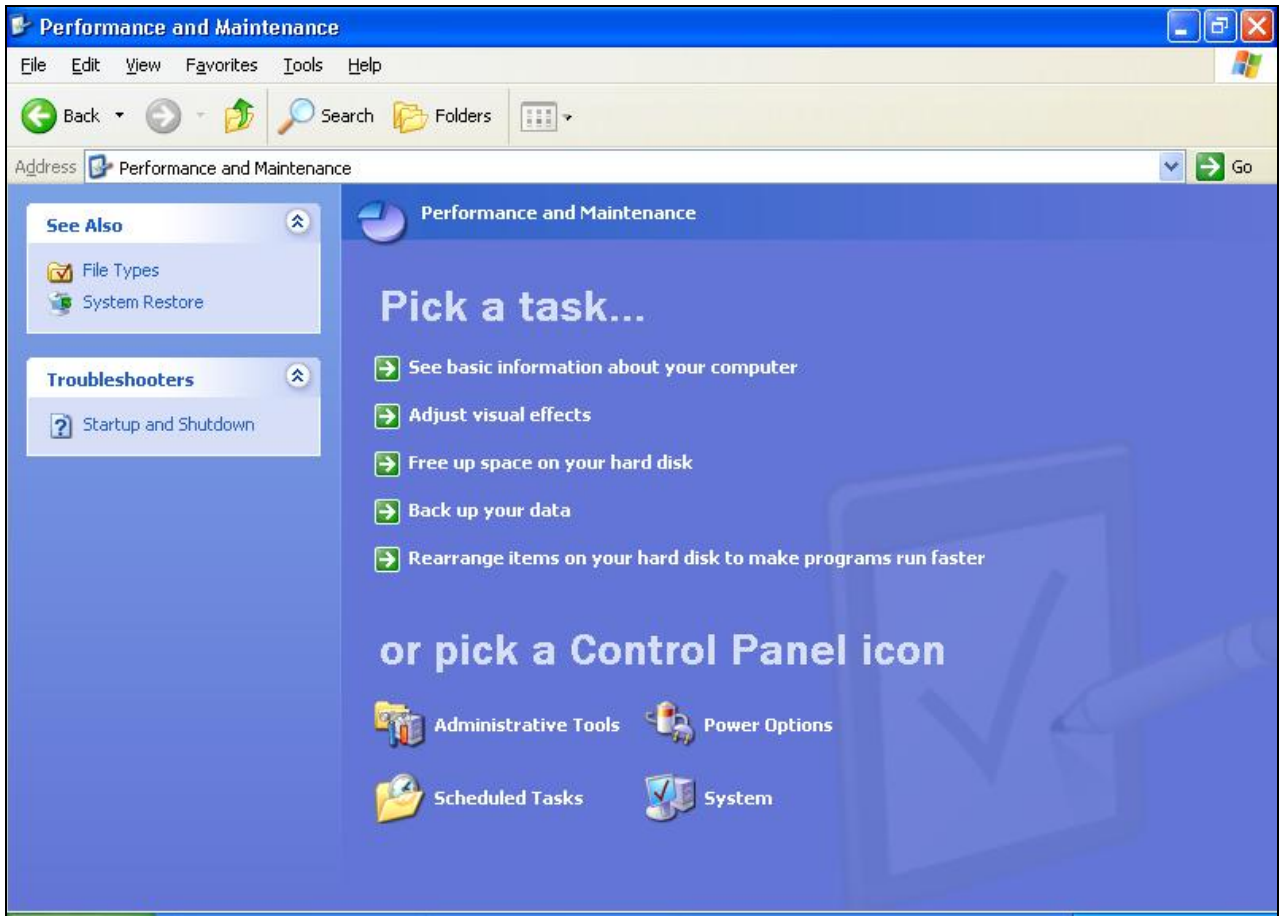
(Configuration on WIN 2000 is similar to XP)

1. On Win 2000/XP, click [Start] button, select [Run], type **secpol.msc** in the field, then click [Run]→ Goto ****Local Security Policy Settings**** page

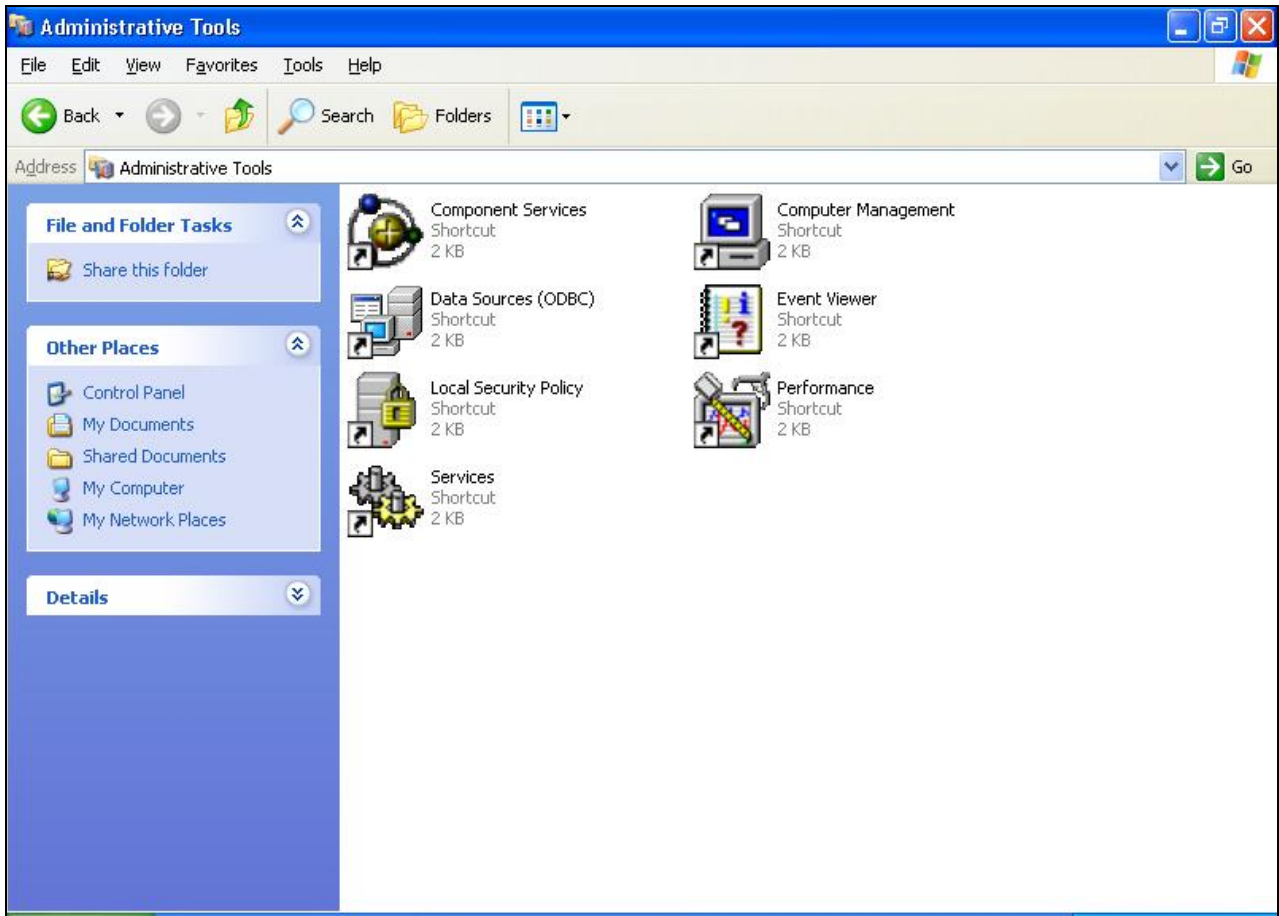
2. Or in Win XP, Click [Control Panel]



Double-click [Performance and Maintenance]

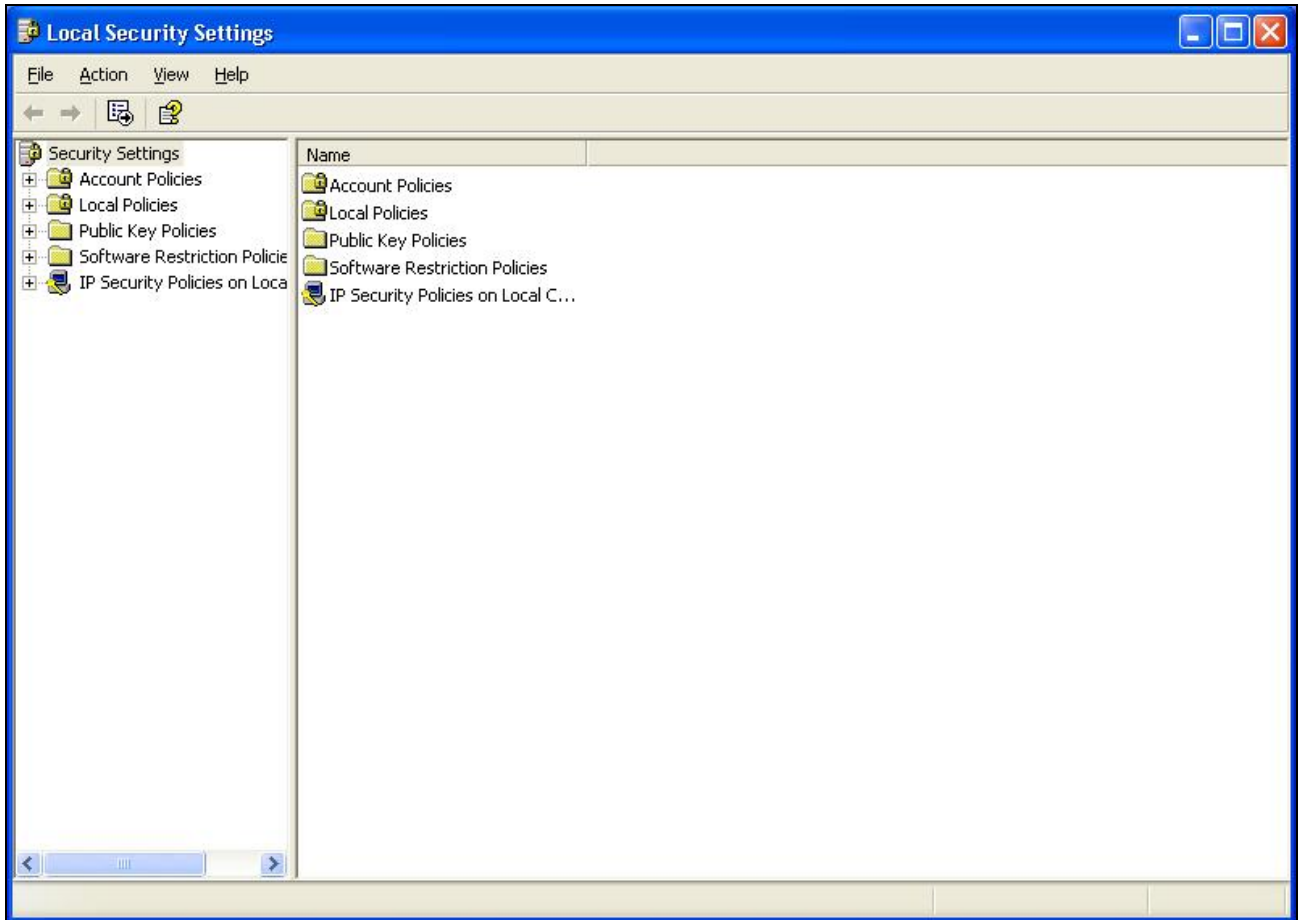


Double-click [Administrative Tools]



Local Security Policy Settings

Double-click [Local Security Policy]

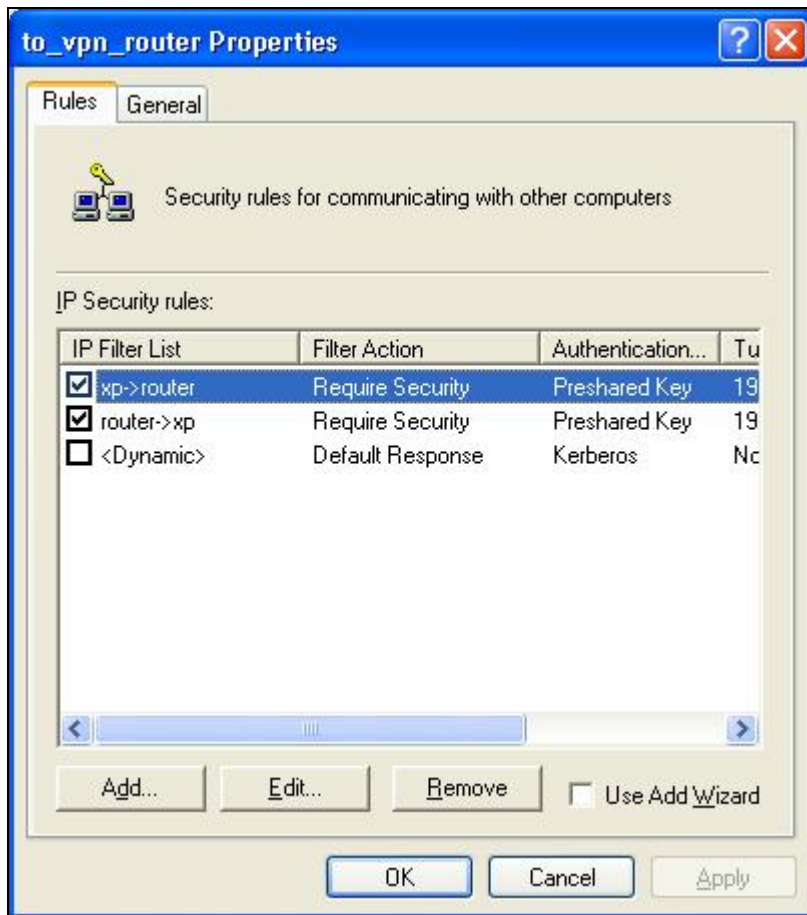


Right-click **[IP Security Policies on Local Computer]**, and click **[Create IP Security Policy]**.

Click the **[Next]** button, enter your policy's name (Here it is **to_vpn_router**). Then, click **[Next]**.

Dis-select the **[Activate the default response rule]** check box, and click **[Next]** button.

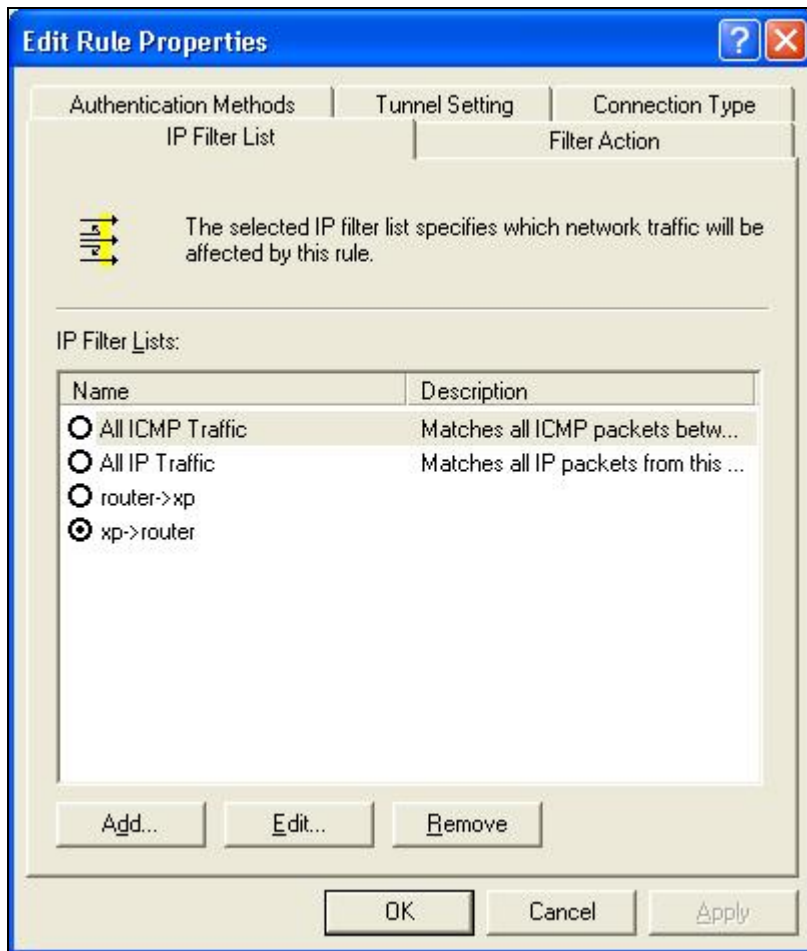
Click **[Finish]** button, make sure **[Edit]** check box is checked.



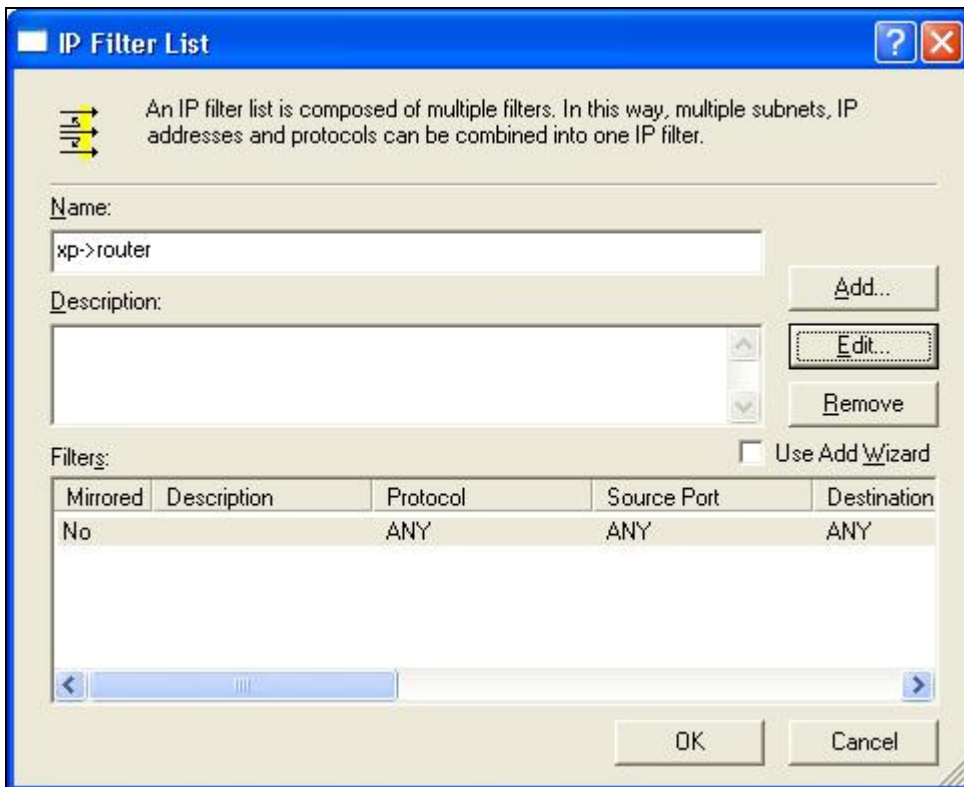
Build 2 Filter Lists: “xp->router” and “router->xp”

Filter List 1: xp-> router

In the “new policy’s properties” screen, select [Use Add Wizard] check box, and then click [Add] button to create a new rule.

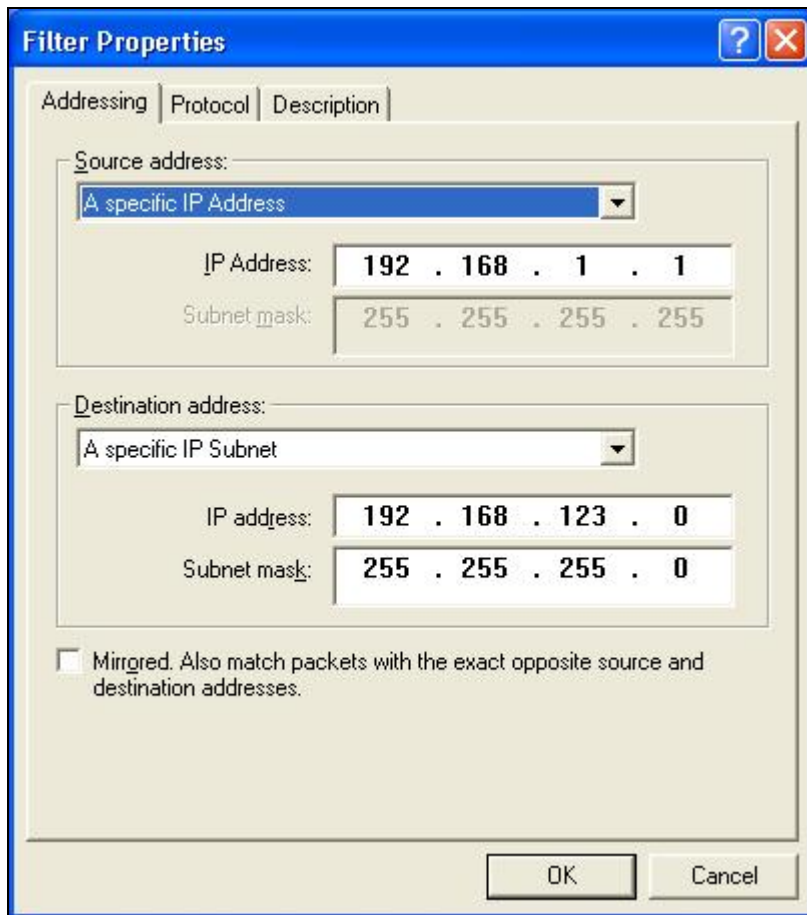


click **[Add]** button



Enter a name, for example: **xp->router**

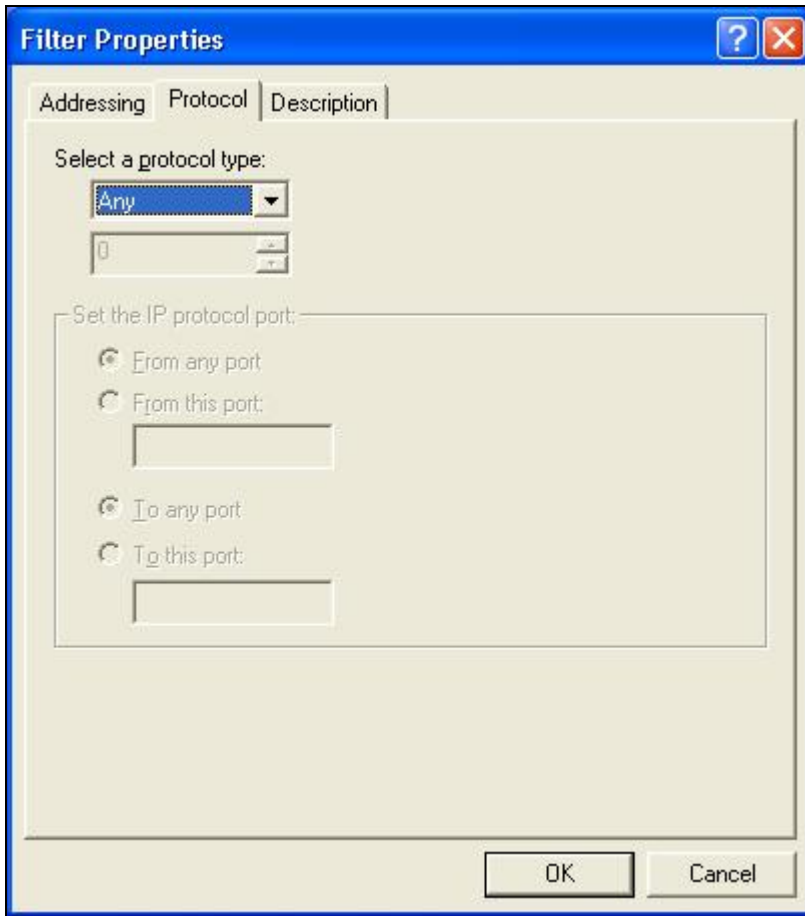
and dis-select [Use Add Wizard] check box. Click [Add] button.



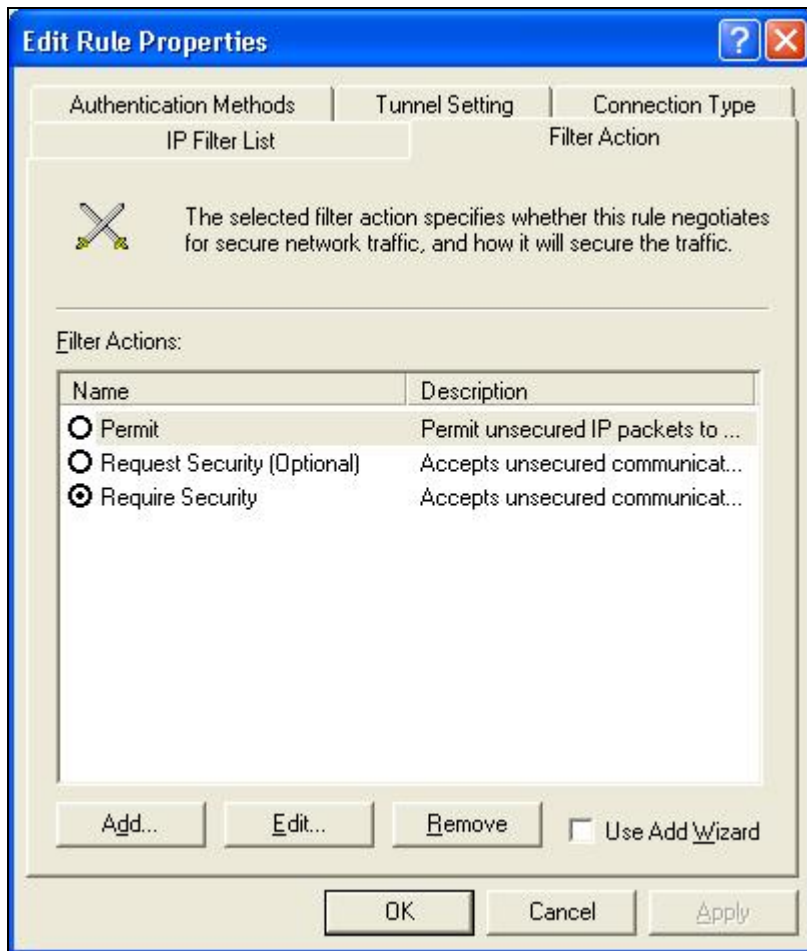
In the Source address field, select [**A specific IP Address**].
and fill in IP Address: **192.168.1.1**

In the Destination address field, select [**A specific IP Subnet**], fill in
IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

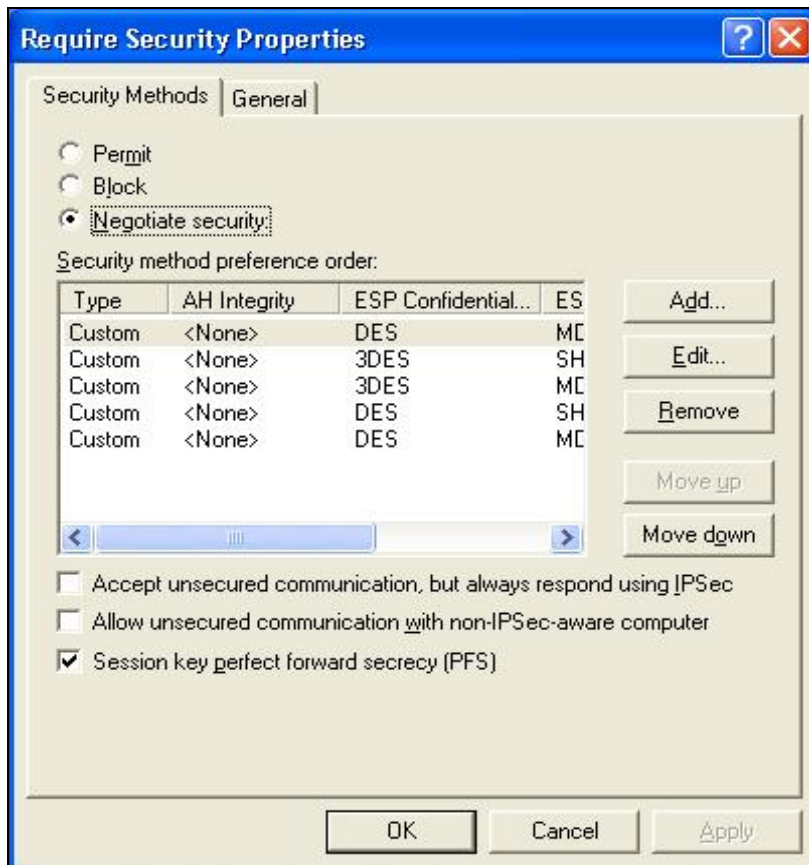
If you want to select a protocol for your filter, click [**Protocol**] page.



Click **[OK]** button. Then click **[OK]** button on the “**IP Filter List**” page.

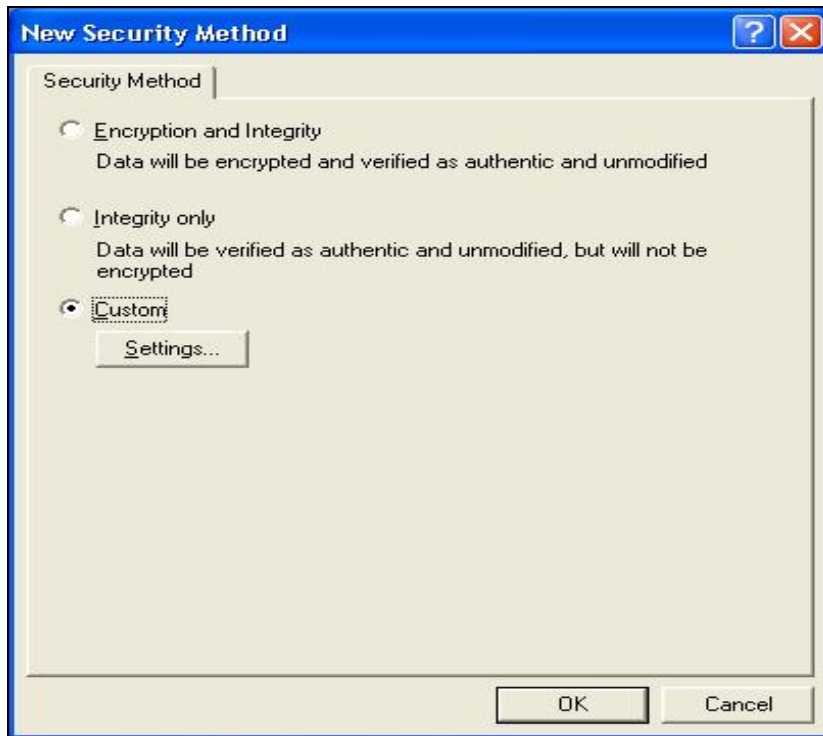


select **[Filter Action]**, select **[Require Security]**, then click **[Edit]** button.

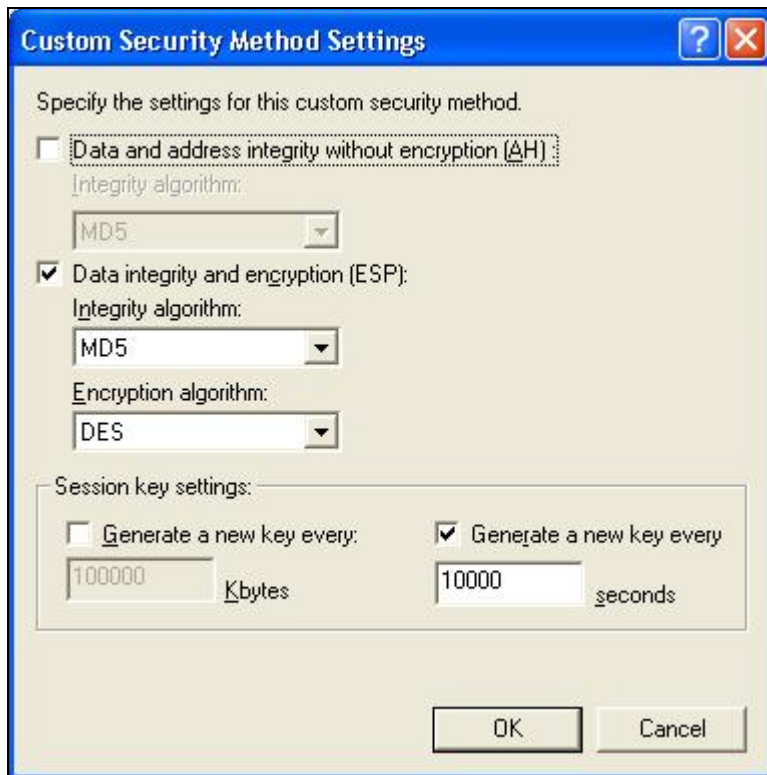


select **[Negotiate security]**, Select **[Session key Perfect Forward Secrecy (PFS)]**

click **[Edit]** button.



select [**Custom**] button



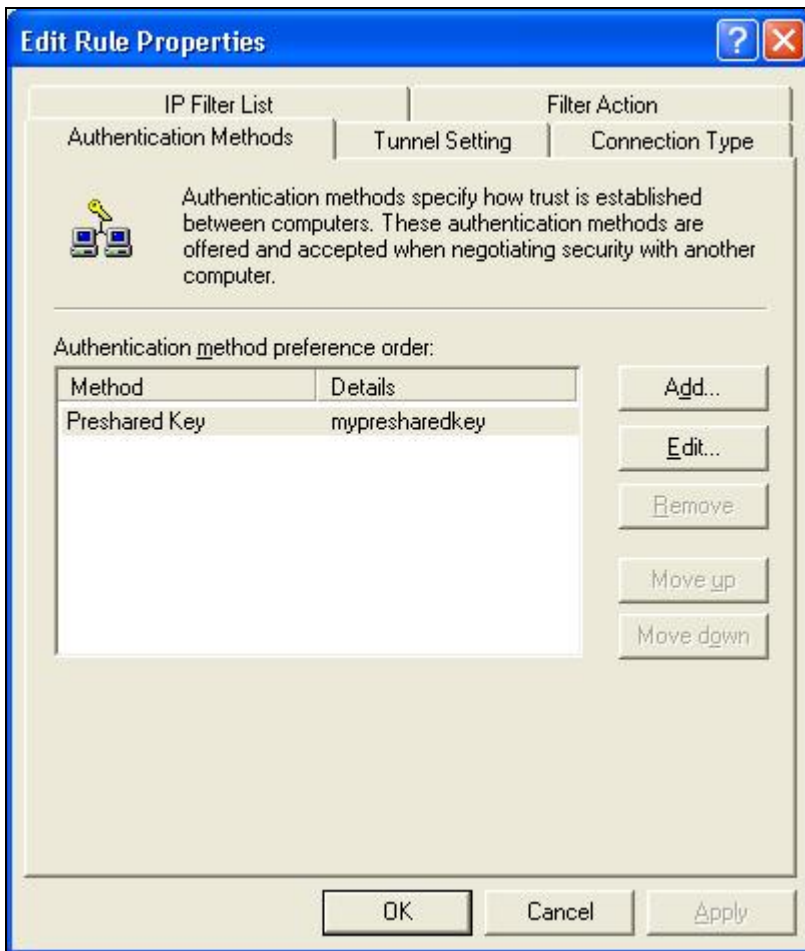
Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

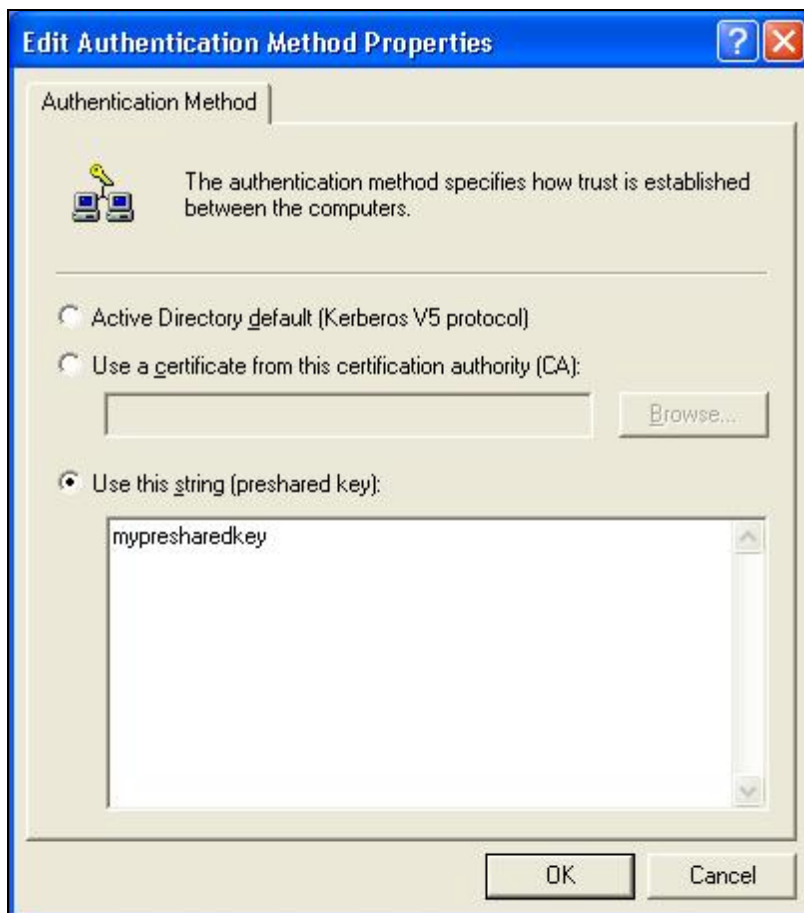
Configure “**Encryption algorithm**”: **[DES]**

Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button



select **[Authentication Methods]** page, click **[Add]** button.



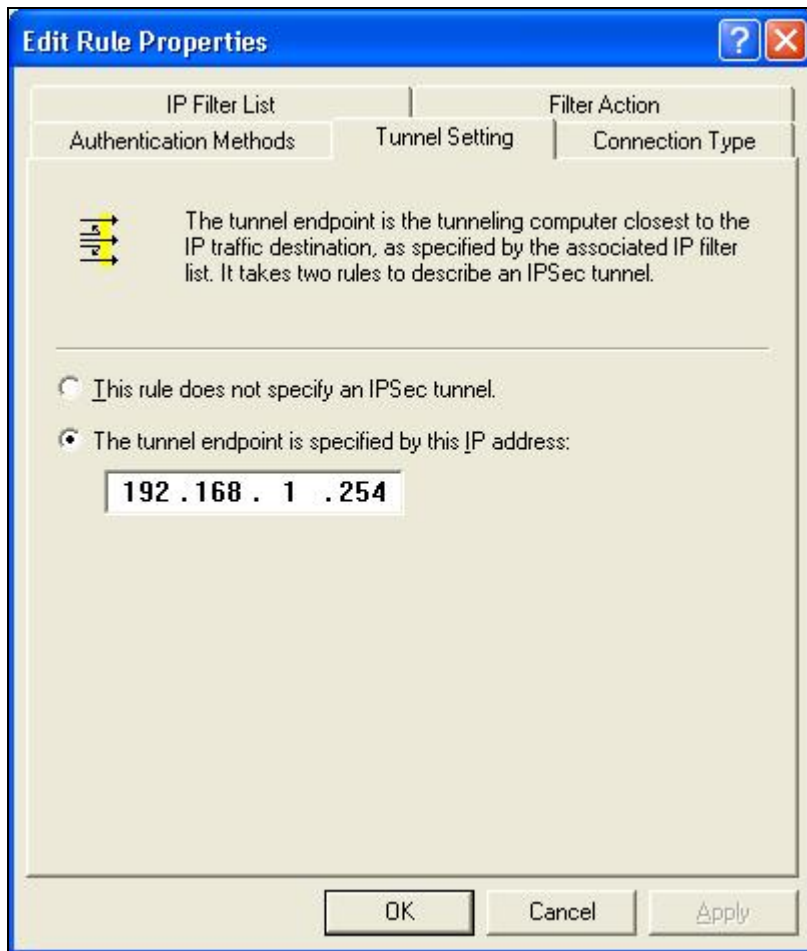
select **[Use this string to protect the key exchange (pre-shared key)]**,

and enter your pre-shared key string, such as

mypresharedkey. Click **[OK]** button.

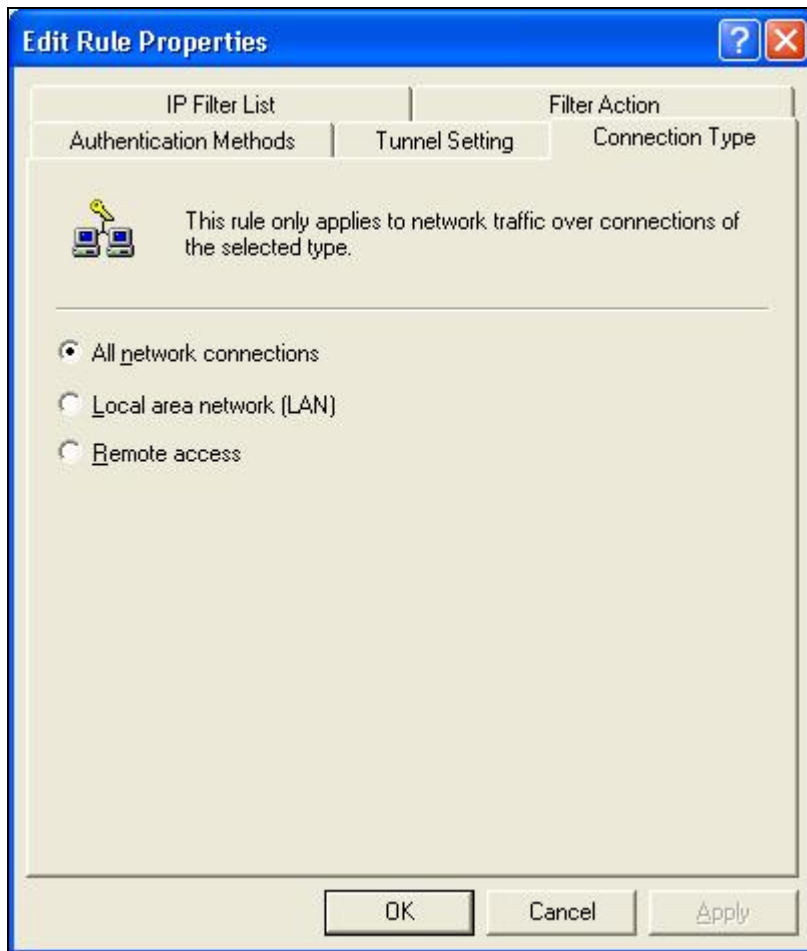
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



configure **[The tunnel endpoint is specified by this IP address]: 192.168.1.254**

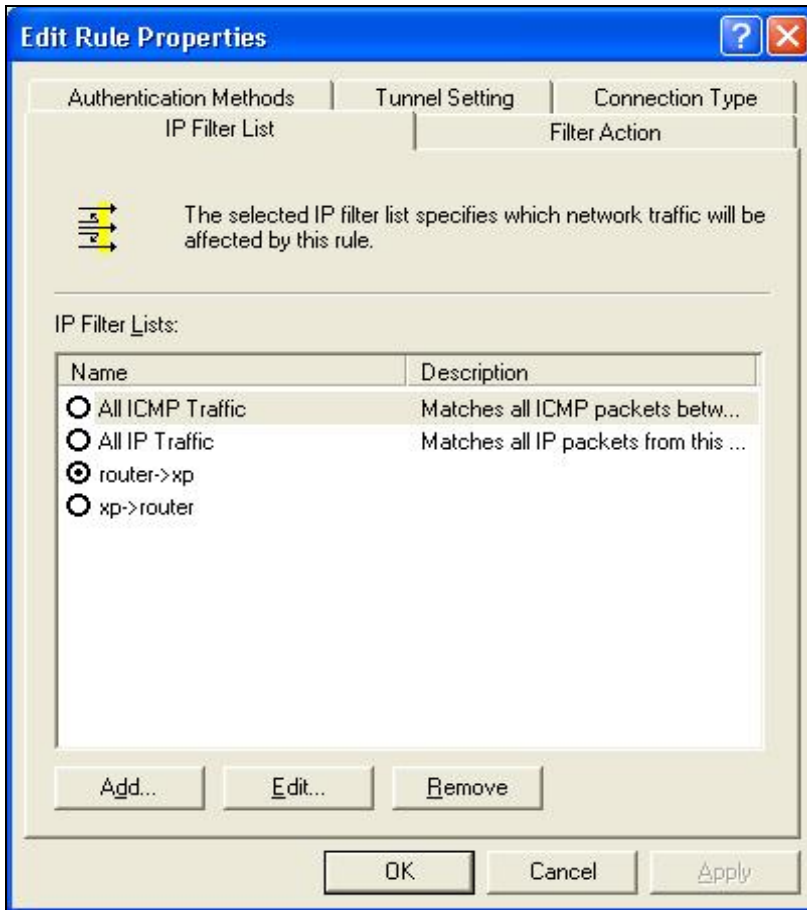
Select **[Connection Type]**



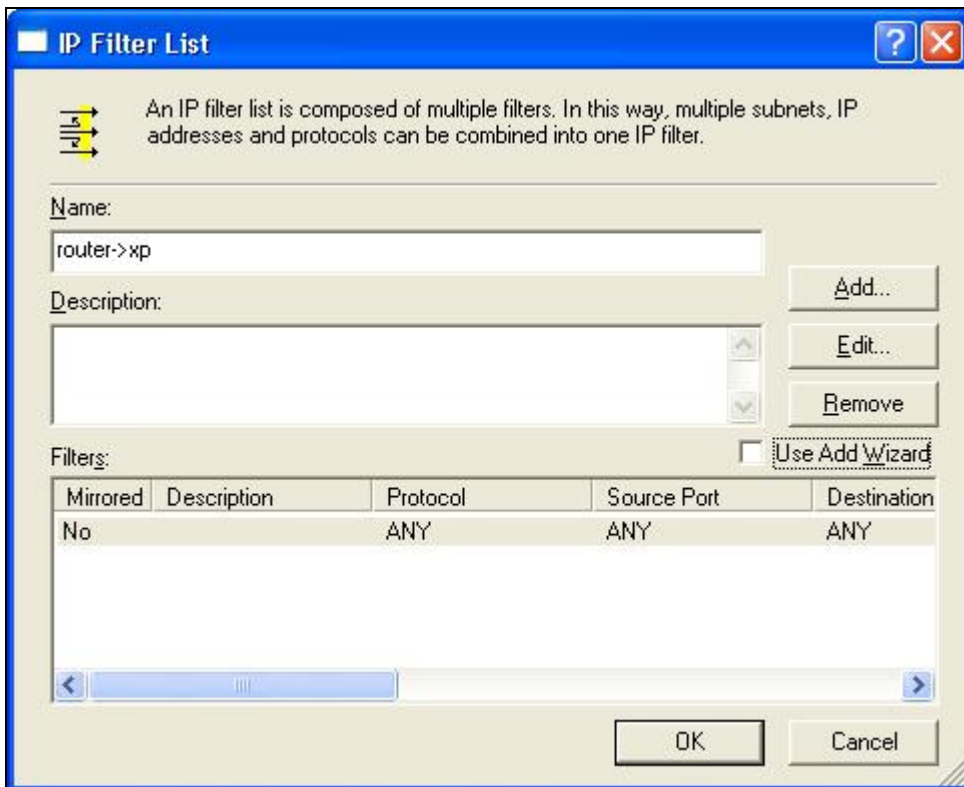
select [**All network connections**]

Tunnel 2: router->xp

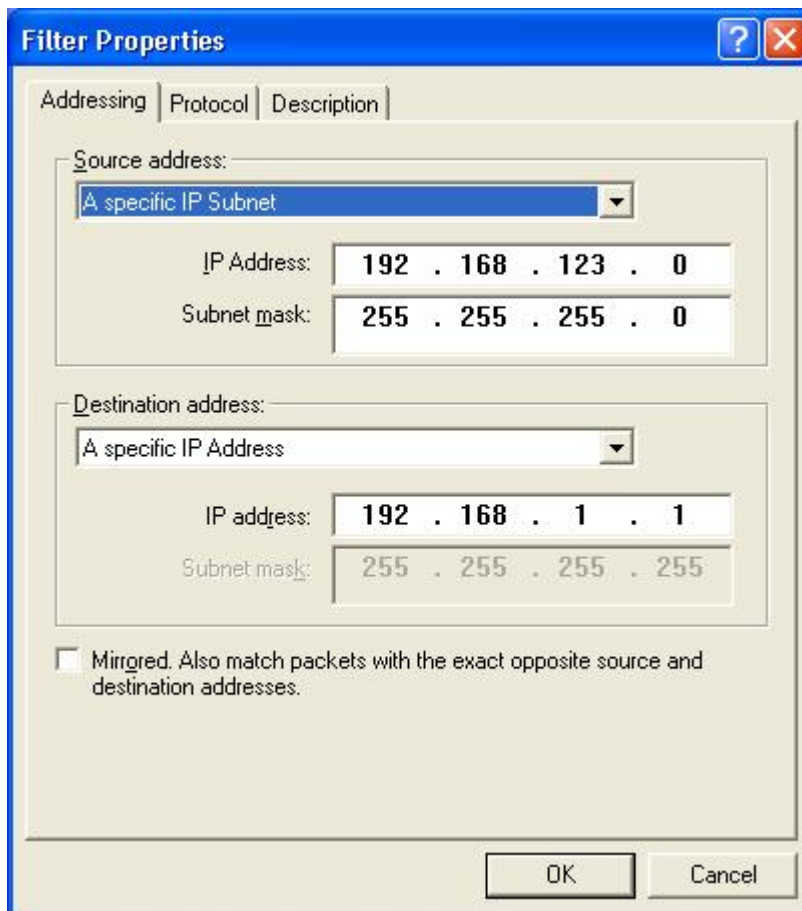
In the “**new policy’s properties**” page, dis-select [**Use Add Wizard**] check box, and then click [**Add**] button to create a new rule.



click **[Add]** button



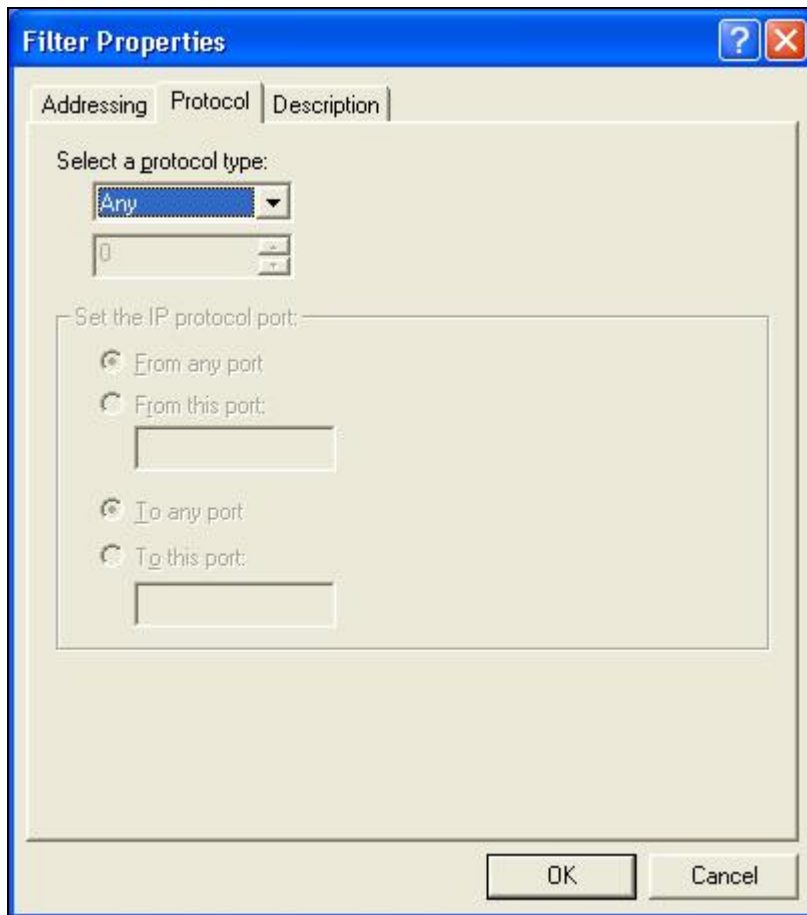
Enter a name, such as **router->xp**
and dis-select [Use Add Wizard] check box. Click [Add] button.



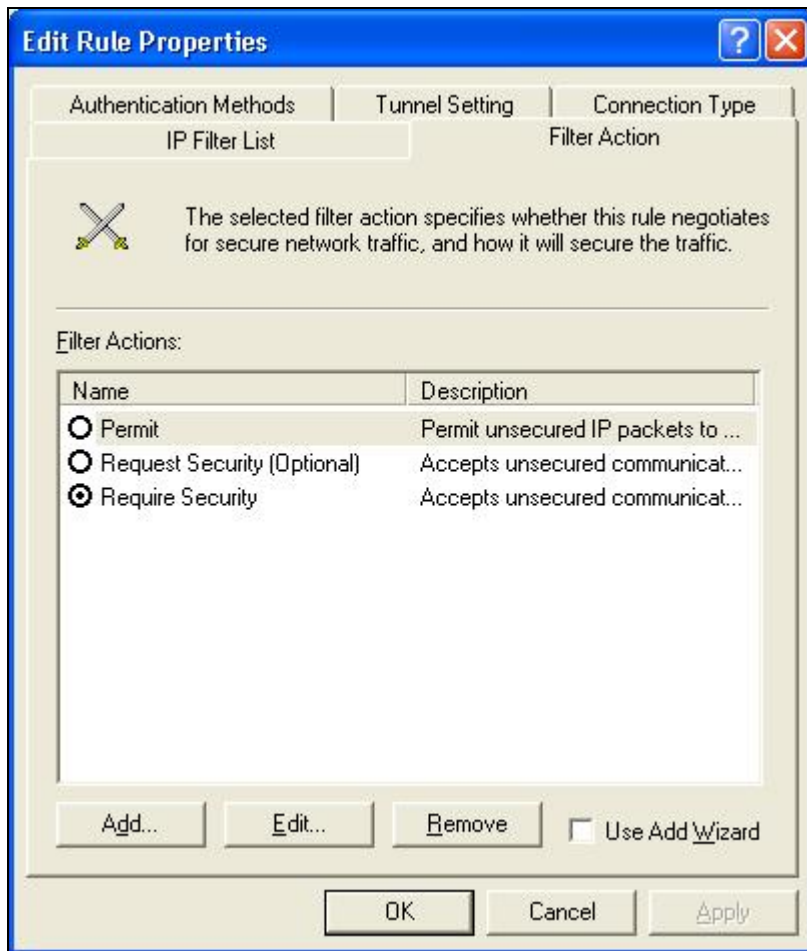
In the Source address field, select [**A specific IP Subnet**]. fill in IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

In the Destination address field, select [**A specific IP Address**], and fill in IP Address: **192.168.1.1**

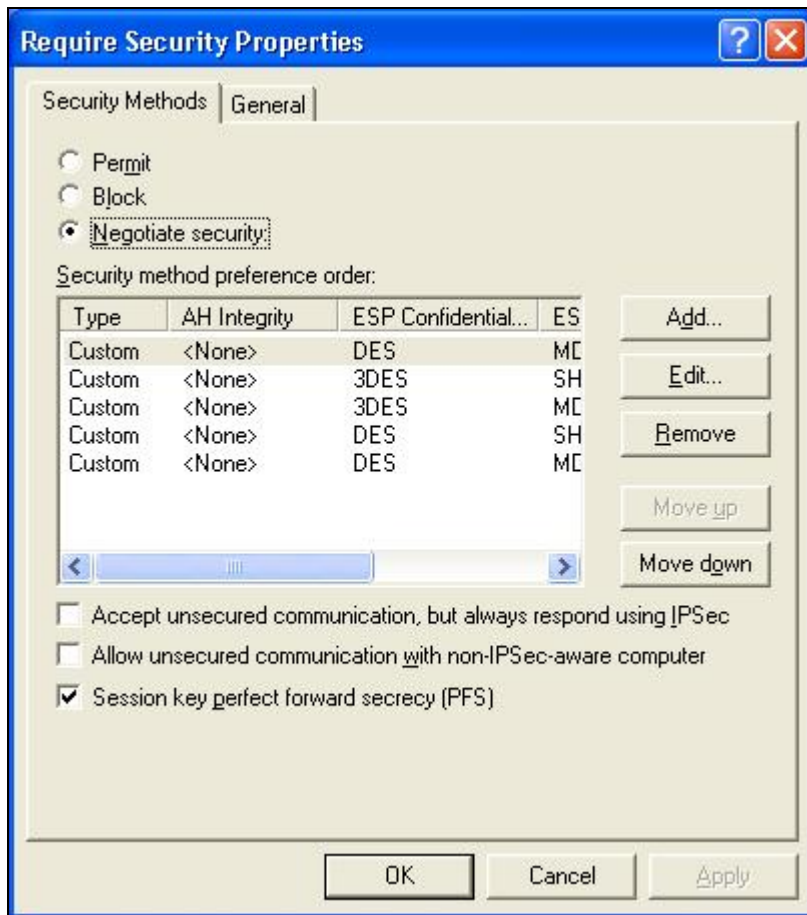
If you want to select a protocol for your filter, click [**Protocol**] page.



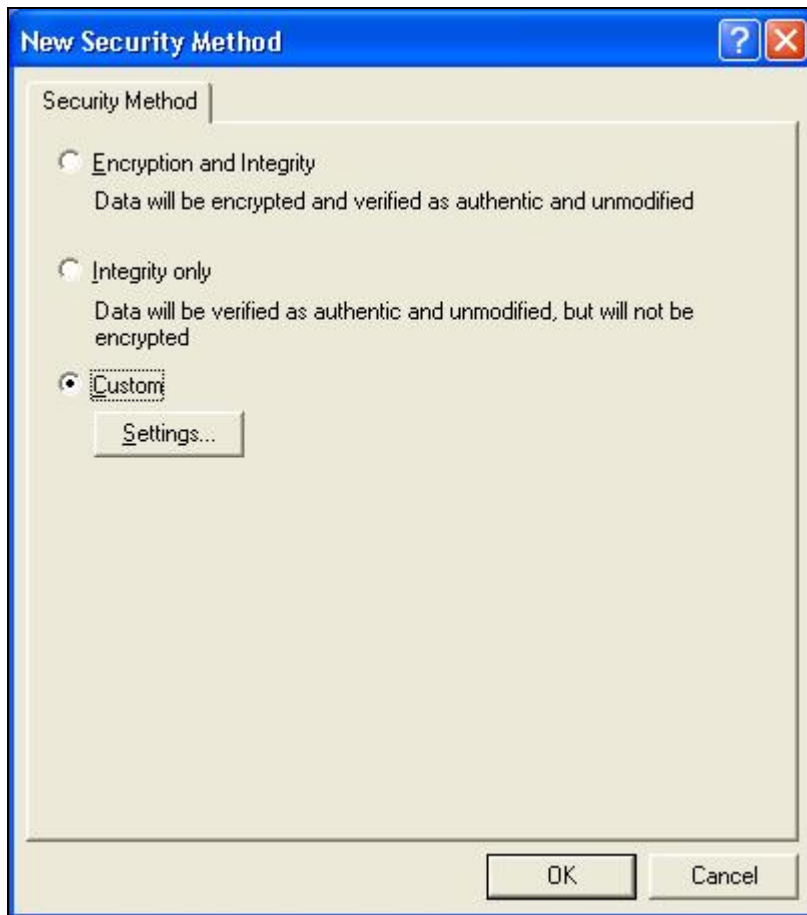
Click **[OK]** button. Then click **[OK]** button on **[IP Filter List]** window.



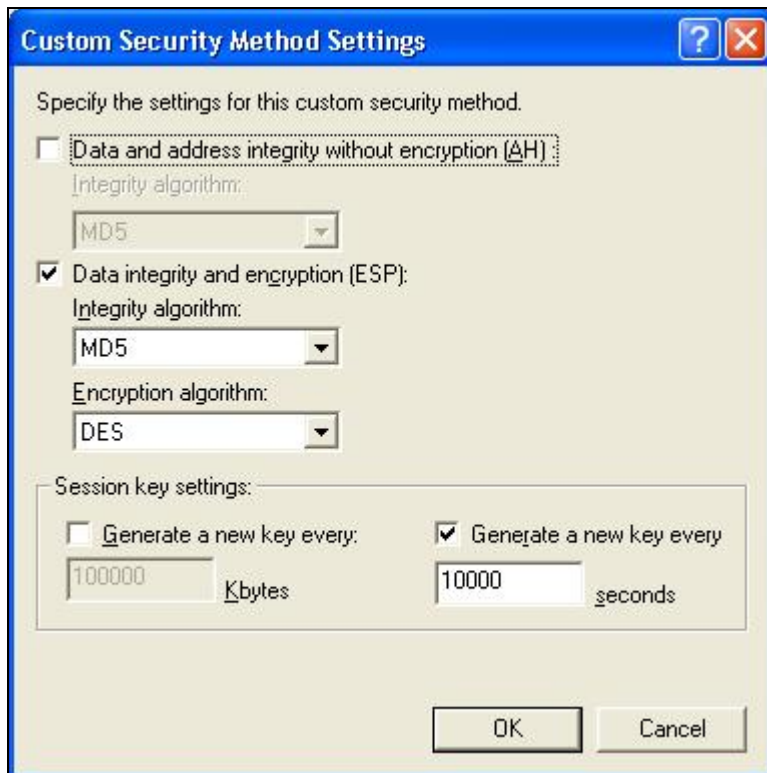
select **[Filter Action tab]**, select **[Require Security]**, then click **[Edit]** button.



select **[Negotiate security]**, Select **[Session key Perfect Forward Secrecy (PFS)]**
click **[Edit]** button.



select [**Custom**] button



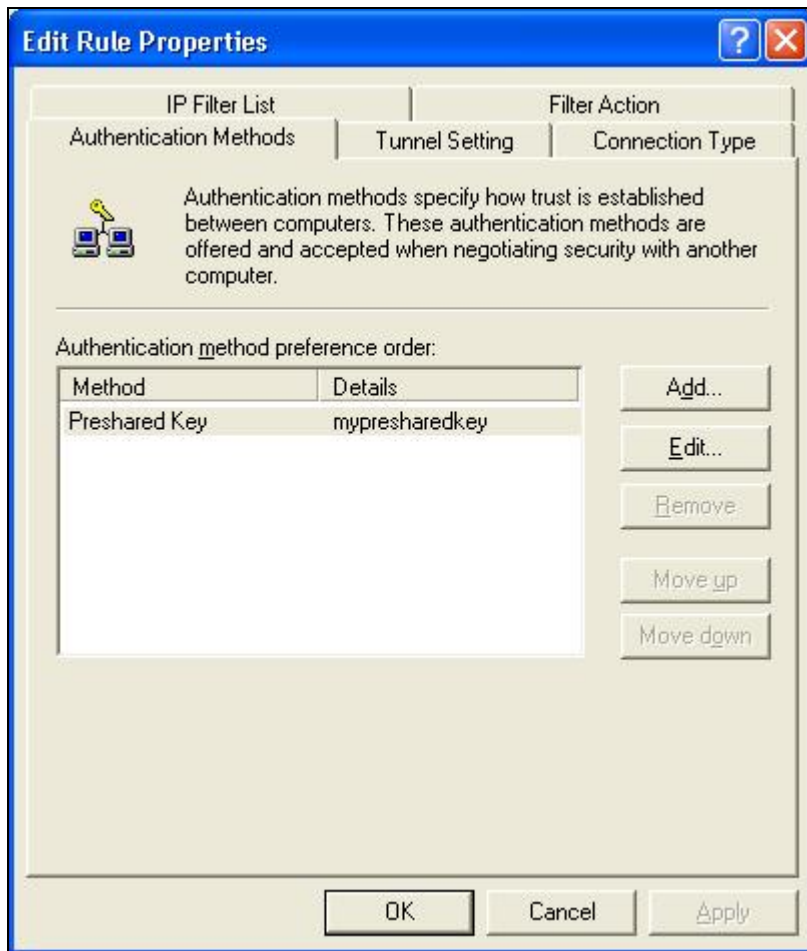
Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

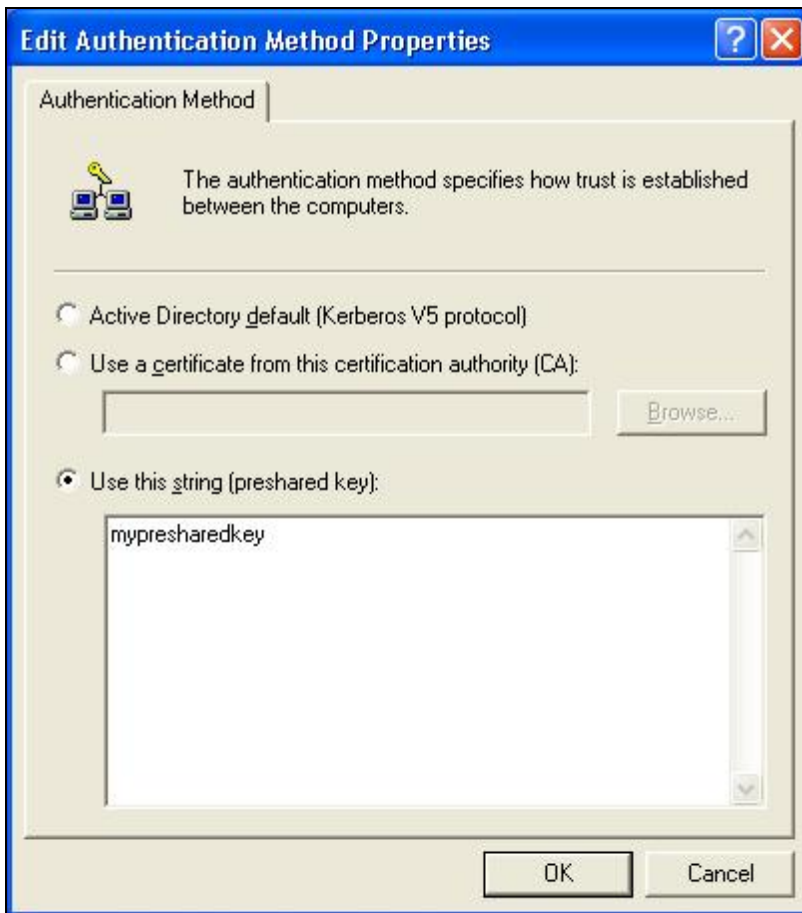
Configure “**Encryption algorithm**”: **[DES]**

Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button



select **[Authentication Methods]** page, click **[Add]** button.



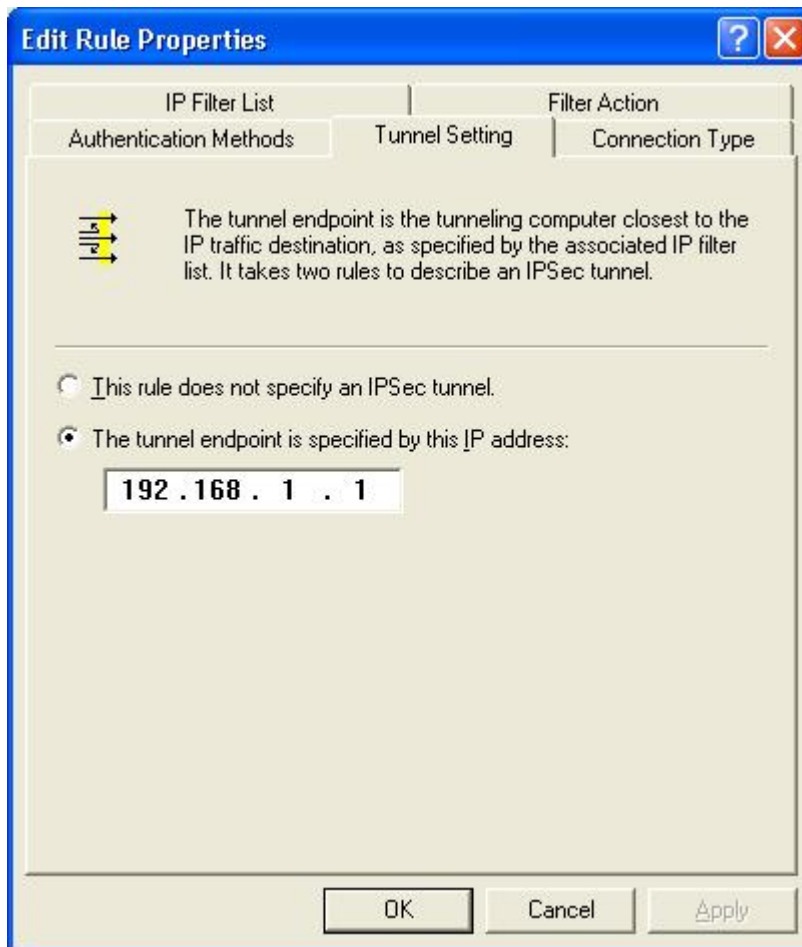
select **[Use this string to protect the key exchange (pre-shared key)]**,

and enter the pre-shared key string, such as

mypresharedkey. Click **[OK]** button.

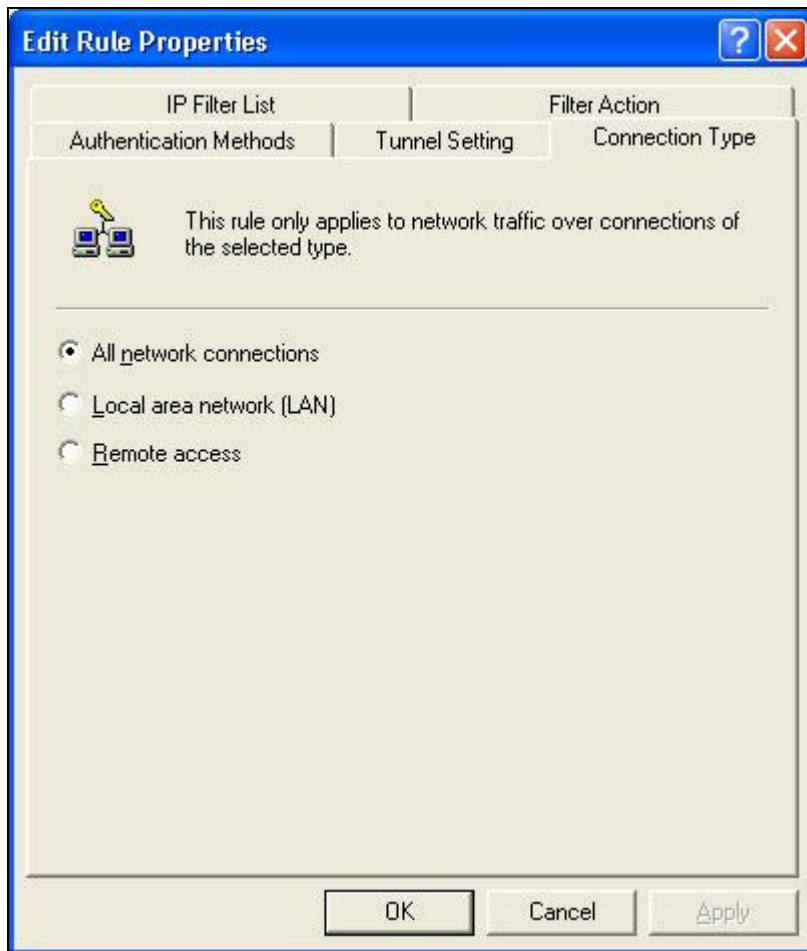
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



Configure [**The tunnel endpoint is specified by this IP address**]: **192.168.1.1**

Select [**Connection Type**]



select [All network connections]

Configure IKE properties

Select **[General]**



Click **[Advanced...]**



enable “**Master key perfect forward security (PFS)**”

configure “**Authenticate and generate a new key after every [10000] seconds**”

click [**Methods...**]



click [**Add**] button



Configure “**Integrity algorithm**”: [SHA1]

Configure “**Encryption algorithm**”: [3DES]

Configure “**Diffie-Helman group**”: [Medium (2)]

Settings on VPN router

VPN Router: Wan IP address:192.168.1.254

Lan IP address:192.168.123.254

PC: 192.168.123.123

level one
BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Setting

- Packet Filters
- Domain Filters
- MAC Address Control
- VPN
- Miscellaneous

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	<input type="text" value="2"/>

ID	Tunnel Name	Method
1	<input type="text" value="1"/>	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>

Current Time
01/12/2004 15:29:25

<< Previous Next >> Save Undo Dynamic VPN Settings... Help

VPN Settings:

VPN: Enable

Max. number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Press "More" →

level one BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Setting

- Packet Filters
- Domain Filters
- MAC Address Control
- VPN
- Miscellaneous

Current Time: 01/12/2004 15:31:24

VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	1
Local Subnet	192.168.123.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.1
Remote Netmask	255.255.255.255
Remote Gateway	192.168.1.1
Preshare Key	mypresharekey
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Save Undo Back Help Reboot

Saved! Items marked with > don't take effective until rebooting!

VPN Settings - Tunnel 1 – IKE

Tunnel:1

Local Subnet:192.168.123.0

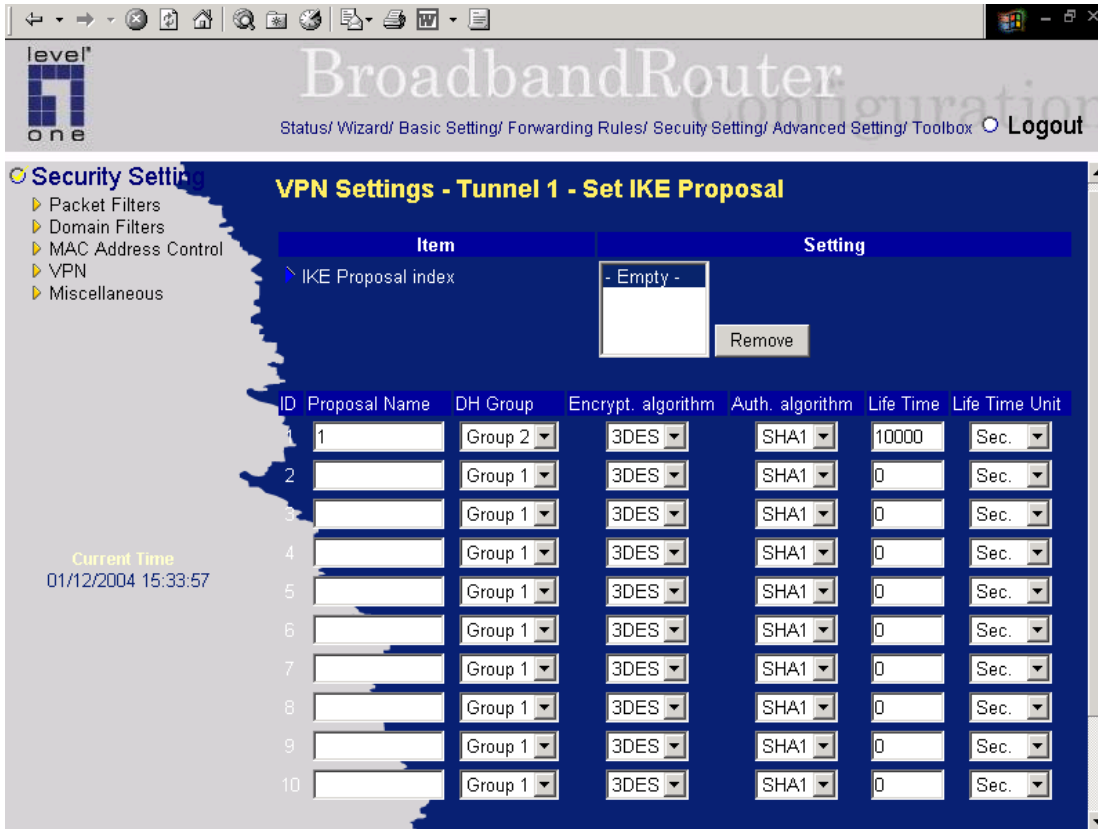
Local Netmask:255.255.255.0

Remote Subnet:192.168.1.1

Remote Netmask:255.255.255.255

Remote Gateway:192.168.1.1

Preshare Key: my-preshare-key



VPN Settings - Tunnel 1 - Set IKE Proposal

ID: 1

Proposal Name: 1

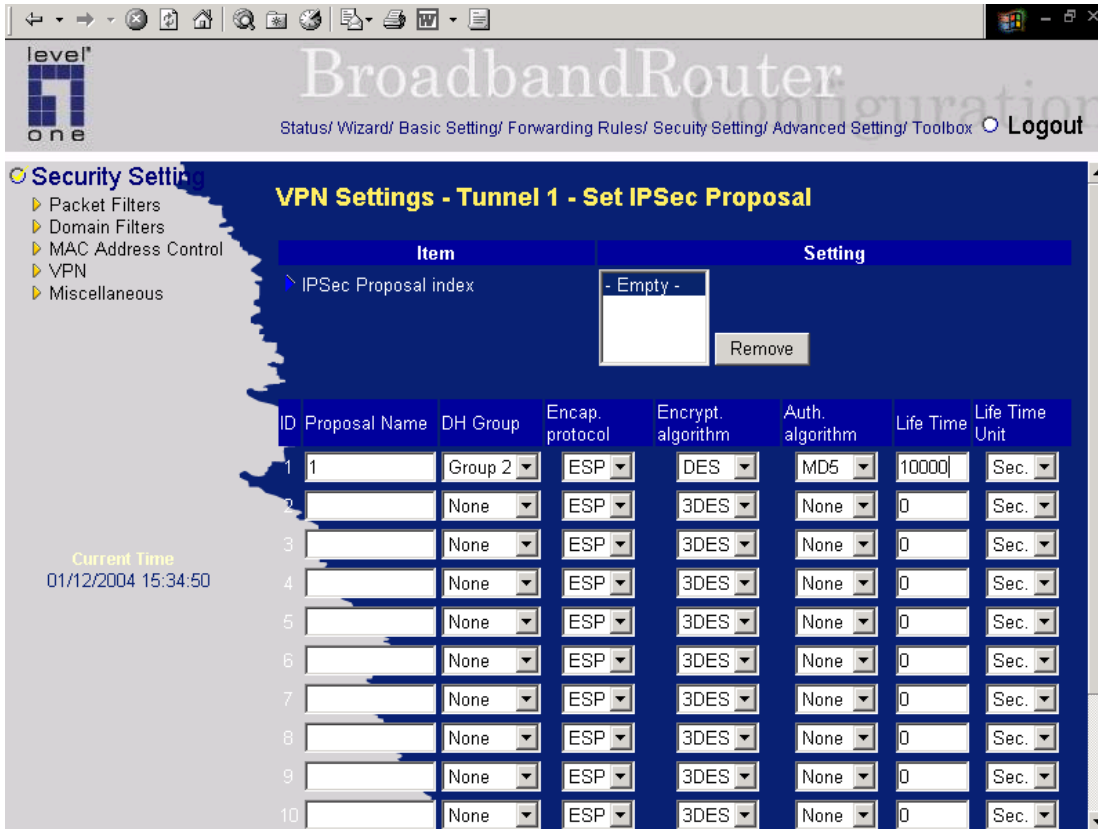
DH Group: Group2

Encrypt. Algorithm: 3DES

Auth. Algorithm: SHA1

Life Time: 10000

Life Time Unit: Sec.



VPN Settings - Tunnel 1 - Set IPSec Proposal

ID: 1

Proposal Name: proposal1

DH Group: Group2

Encap. Protocol: ESP

Encrypt. Algorithm: DES

Auth. Algorithm:MD5

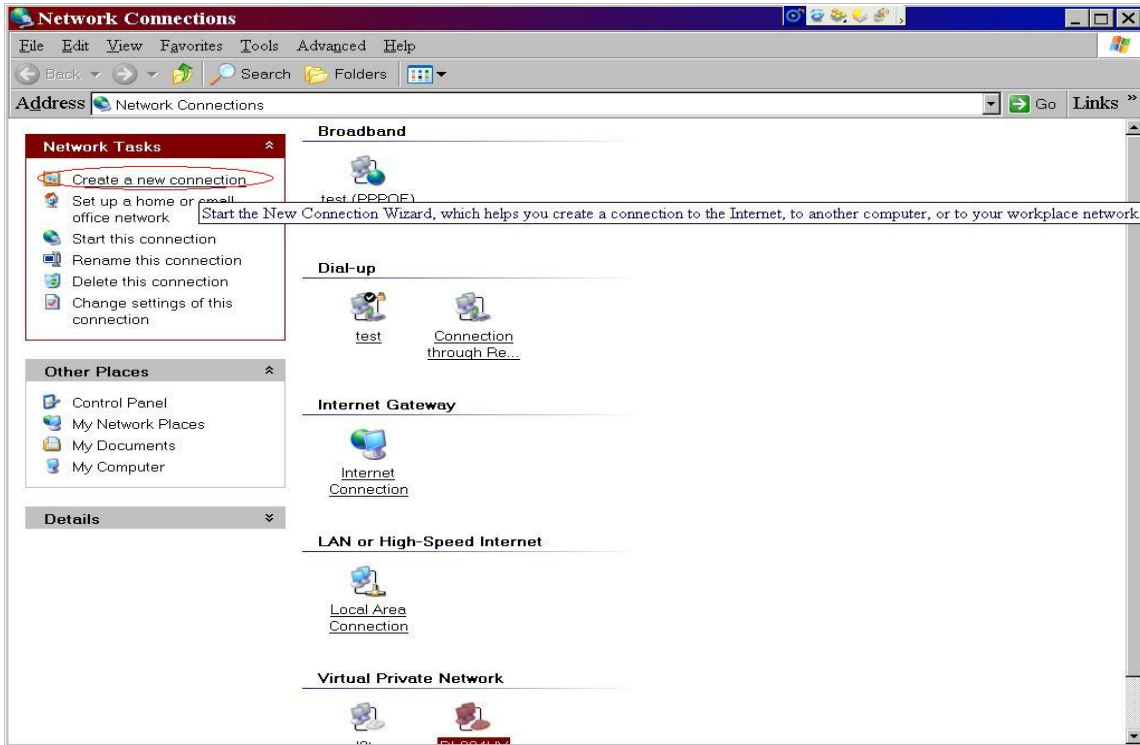
Life Time: 10000

Life Time Unit: Sec.

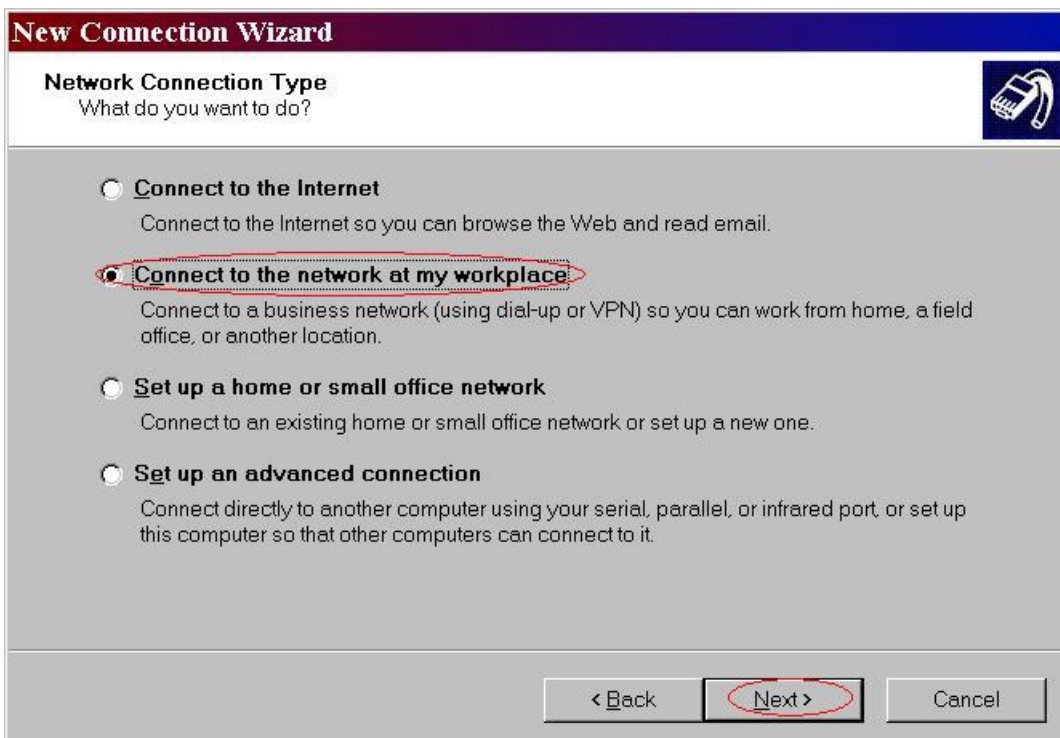
User can view VPN connection process in “**System Log**” page, and correct their settings.

Appendix C PPTP and L2TP Configurations

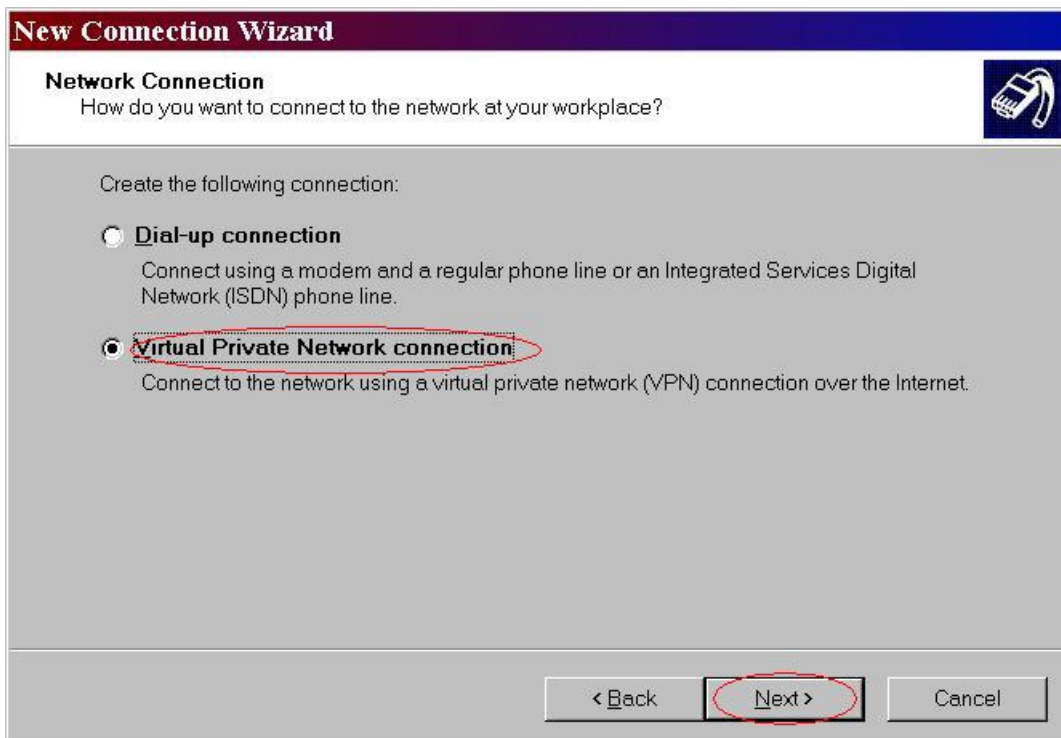
1. First, please go to the Network connection



2. Connect to network at my workplace



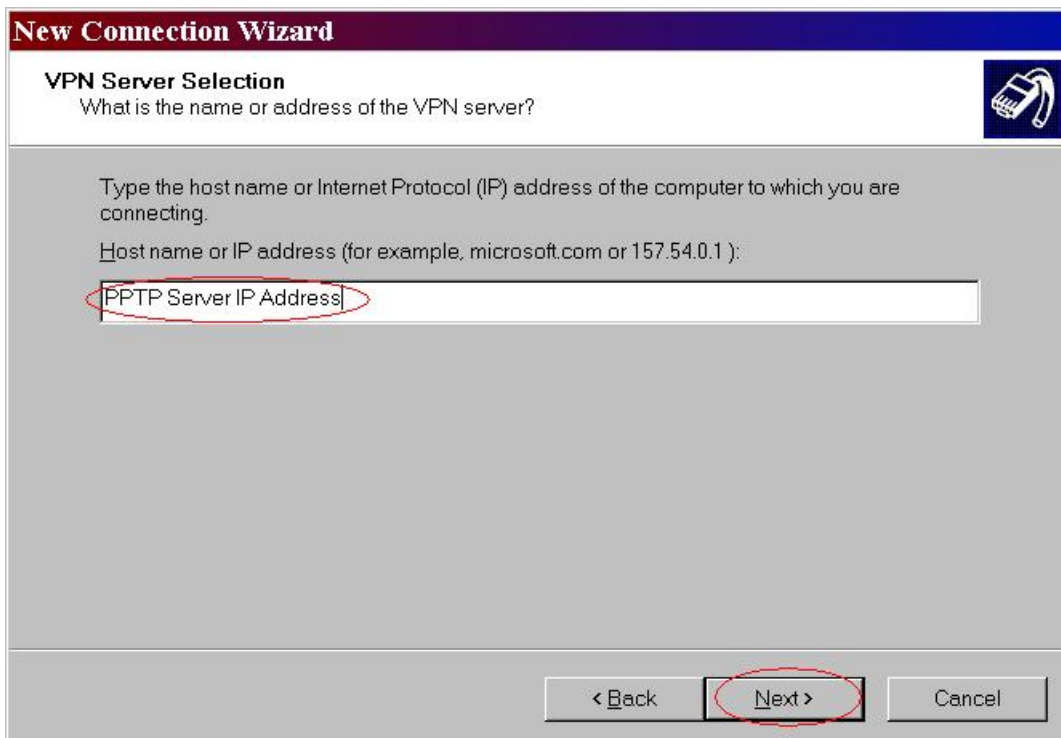
3. Choose Virtual Private Network



4. Do not dial to initial connection



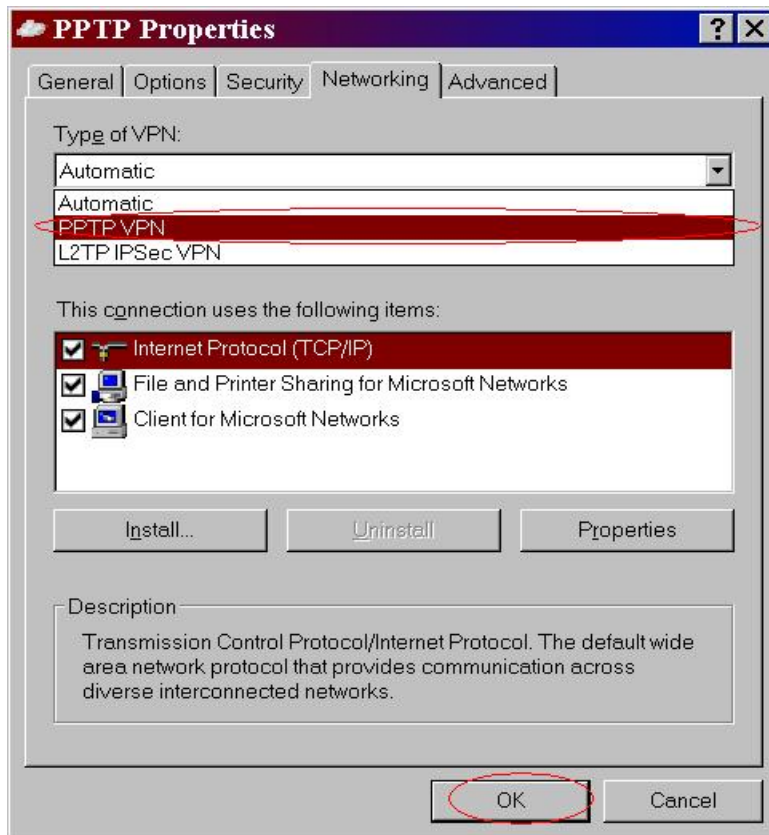
5. Input the router wan ip address



6. Then ok, please input username and password as you setup in the router.



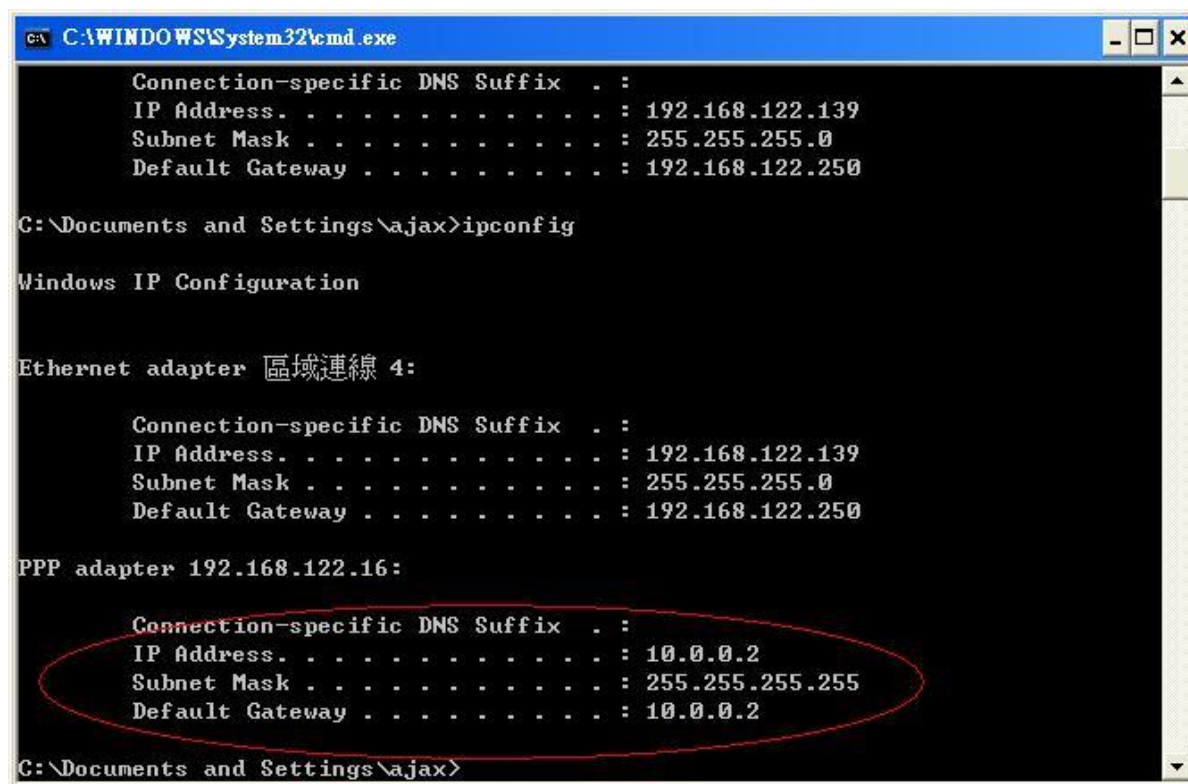
7. Select the type of VPN



However, you should add the Authentication Protocol in advanced(Custom setting) of Security option, like below to support pap, chap, mschap.

If successfully, we will see:

This time, the client in the internet can ping any pcs in the lan(192.168.123.x)



```
C:\WINDOWS\System32\cmd.exe

Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.122.139
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.122.250

C:\Documents and Settings\ajax>ipconfig

Windows IP Configuration

Ethernet adapter 區域連線 4:

    Connection-specific DNS Suffix . :
    IP Address . . . . . : 192.168.122.139
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.122.250

PPP adapter 192.168.122.16:

    Connection-specific DNS Suffix . :
    IP Address . . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 10.0.0.2

C:\Documents and Settings\ajax>
```

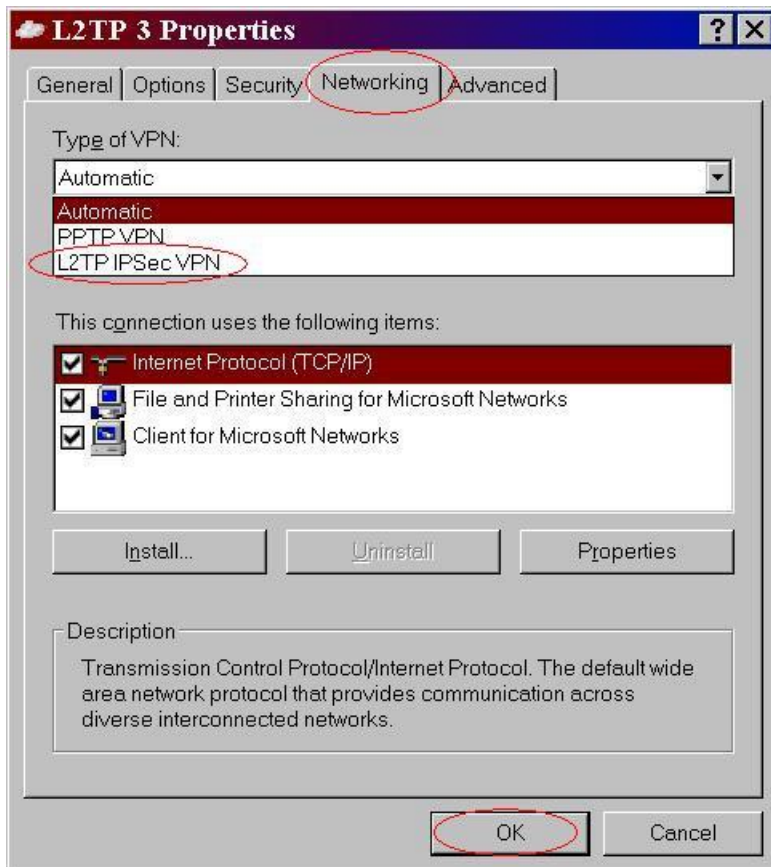
L2TP

However, the router is the also vpn-l2tp server and supports three Authentication Protocols, PAP, CHAP and MSCAP.

And the settings are similar with PPTP. But MS-operating systems, like winxp win2000 will not find The type of vpn “L2tp”.We can use this files(disableipsec.zip) to enable it.

<http://support.iglou.com/fom-serve/cache/473.html>

Then We will see L2tp IPSEC VPN and choose it:



Then the steps refer to pptp settings.

Appendix D 802.1x Setting

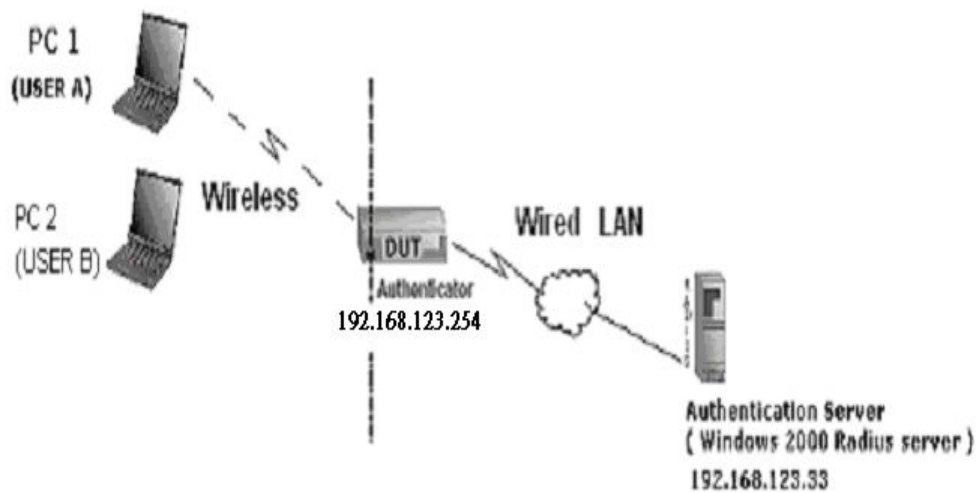


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

1 Equipment Details

PC1:

Microsoft Windows XP Professional without Service Pack 1.

D-Link DWL-650+ wireless LAN adapter

Driver version: 3.0.5.0 (Driver date: 03.05.2003)

PC2:

Microsoft Windows XP Professional with Service Pack 1a.

Z-Com XI-725 wireless LAN USB adapter

Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 (You can get more information from <http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>)

2 DUT

Configuration:

- 1.Enable DHCP server.
- 2.WAN setting: static IP address.

3.LAN IP address: 192.168.123.254/24.

4.Set RADIUS server IP.

5.Set RADIUS server shared key.

6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

3. DUT and Windows 2000 Radius Server Setup

3-1-1. Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

3-1-2. Setup DUT

- 1.Enable the 802.1X (check the “Enable checkbox“).
- 2.Enter the RADIUS server IP.
- 3.Enter the shared key. (The key shared by the RADIUS server and DUT).
- 4.We will change 802.1X encryption key length to fit the variable test condition.

3-1-3. Setup Network adapter on PC

- 1.Choose the IEEE802.1X as the authentication method. (Fig 2)

Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

- 2.Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
- 3.If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)
- 4.We will change EAP type to fit the variable test condition.

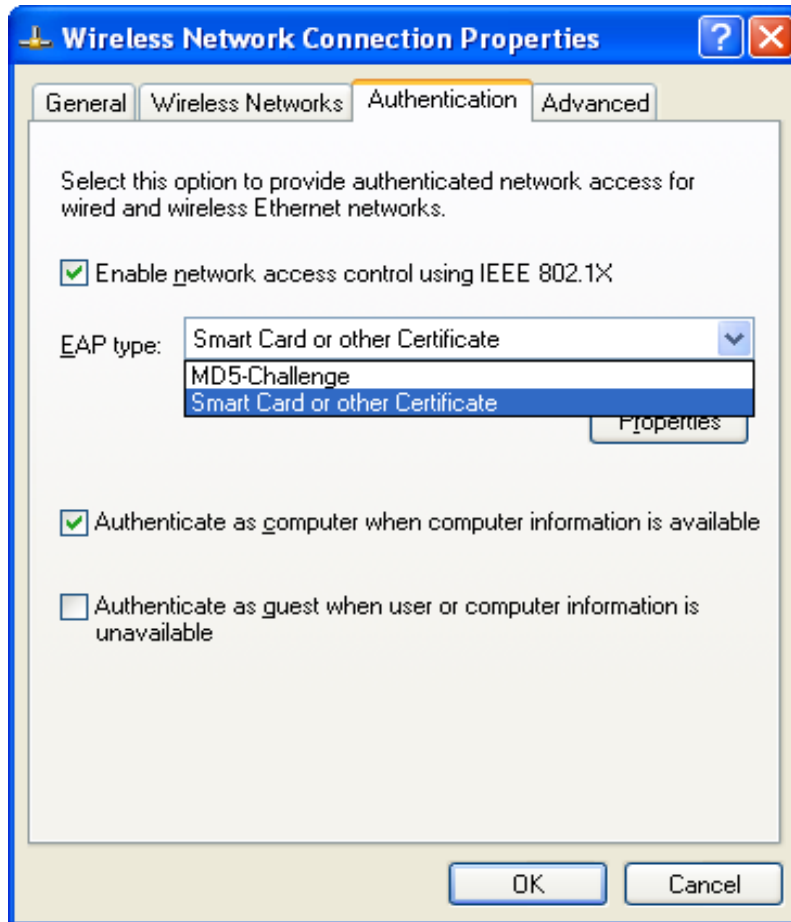


Figure 2: Enable IEEE 802.1X access control

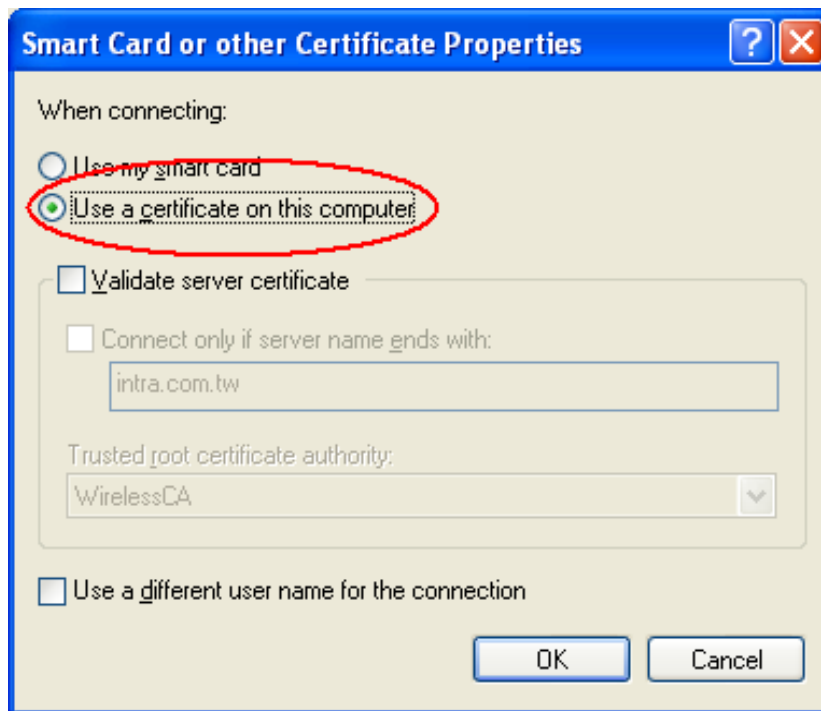


Figure 3: Smart card or certificate properties

4.Windows 2000 RADIUS server Authentication testing:

4.1DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 choose the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

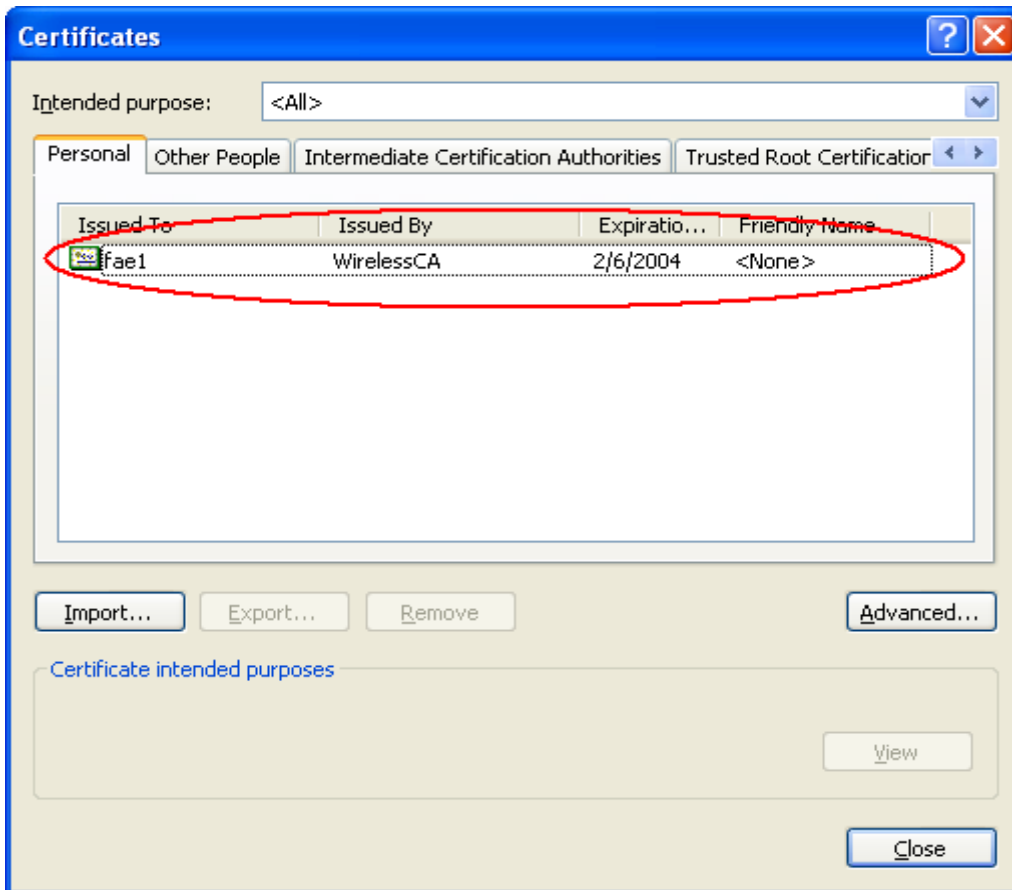


Figure 4: Certificate information on PC1

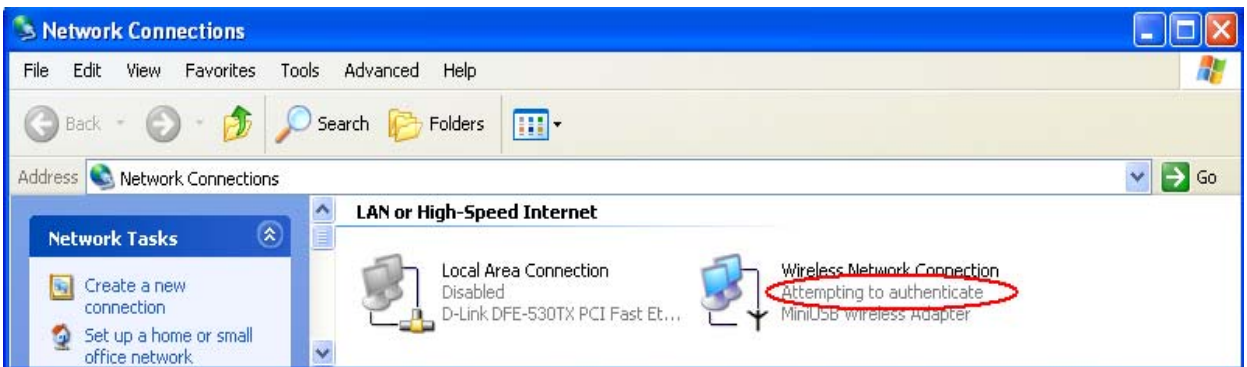


Figure 5: Authenticating

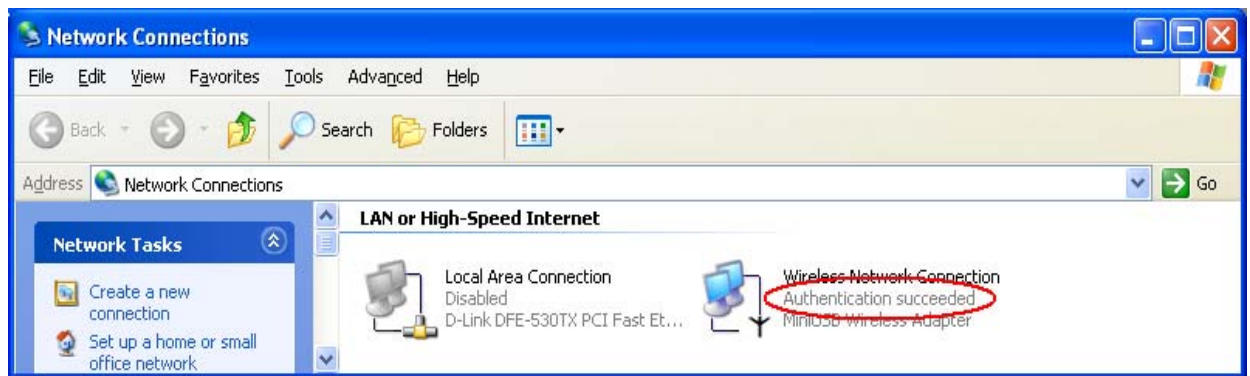


Figure 6: Authentication success

4.2DUT authenticate PC2 using PEAP-TLS.

1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.
- 4.The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

Support Type: Amit supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.

Note.

- 1.PC1 is on Windows XP platform without Service Pack 1.
- 2.PC2 is on Windows XP platform with Service Pack 1a.
- 3.PEAP is supported on Windows XP with Service Pack 1 only.
- 4.Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

Appendix E FAQ and Troubleshooting

Reset to factory Default

There are 2 methods to reset to default.

1. Restore with RESET button

First, turn off the router and press the RESET button in. And then, power on the router and hold the RESET button down until the Status LED start flashing, then move away the hand. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

3. Restore directly when the router power on

First, hold the RESET button about 5 seconds (STATUS LED will start flashing about 5 times),move away the hand. The RESTORE process is completed.

TFTP Mode

1. Symptom: STATUS LED flashes abnormally.

1. STATUS LED flashes very quickly.
2. STATUS LED flashes reciprocally

※We can check if the router works ok or not according to STATUS LED.

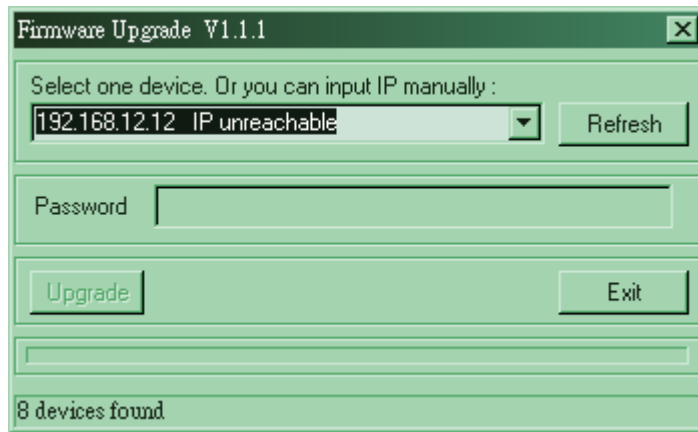
If Normal, the STATUS LED flashes per second.

2. Solution:

1.First execute the execute-file. If the router' address is be found
Please go to the step 3.If not, please go to step2.

2.Turn off the router and press the RESET button in.
And then, power on the router and hold the RESET button down until
the Status LED start flashing.
For a moment the Status LED is flashing very fast
It is Tftp mode.
If failed, please try again.

3. Please use the execute file and click “refresh button”
and will show some devices:



4.If you can find one device and unreachable. You must setup the same submask, For example configure the PC IP address to 192.168.12.xxx.

5. Click “Upgrade Button” and to upgrade the firmware smoothly.

6.If successfully, please use “Reset Button” reset to default the router.
If failed, the program will ask to redo again from Step 2.